PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE JURISPRUDENCIA

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE

ABOGADA

"EL HACKER COMO SUJETO ACTIVO EL DELITO: LIMITES Y EXCEPCIONES DE LA INTROMISION TECNOLÓGICA A LA RED DE INTERNET A LA LUZ DEL CÓDIGO ÓRGANICO INTEGRAL PENAL (COIP)"

MARÍA SUSANA VACA LOAIZA

DIRECTOR: DR. CRISTIAN ZAMBRANO.

QUITO, 2017

EDUARDO LEÓN MICHELI

Quito, 19 de mayo de 2017

Señor doctor
Íñigo Salvador Crespo
Decano de la Facultad de Jurisprudencia
Pontificia Universidad Católica del Ecuador

Señor doctor
Gonzalo Vaca Dueñas
Secretario Abogado de la Facultad de Jurisprudencia
Pontificia Universidad Católica del Ecuador

En contestación al oficio No. 031-SJG-2017, de 11 de abril de 2017, a través del cual se me corrió traslado con la designación de Profesor Informante de la disertación de abogacía titulada "EL HACKER COMO SUJETO ACTIVO DEL DELITO: LÍMITES Y EXCEPCIONES DE LA INTROMISIÓN TECNOLÓGICA EN LA RED DE INTERNET A LA LUZ DEL COIP" de la estudiante María Susana Vaca Loaiza, me permito presentar mi informe en los siguientes términos:

A) La tesis presenta, sin lugar a duda alguna, un tema de investigación de actualidad, de importante relevancia y muy discutido en la realidad nacional. En adición a esta premisa, cabe también resaltar que muy pocos autores a nivel nacional han abordado el tema que la estudiante ha decidido investigar.

B) Los delitos cometidos con el uso de las nuevas tecnologías y los delitos informáticos han sido de aquellos más difíciles de adecuar como infracciones penales autónomas en los ordenamientos jurídicos de la región y en el mundo. Además, otro de los problemas recurrentes desde el inicio del estudio de estas "nuevas" infracciones y medios para delinquir, ha sido el analizar su *iter críminis*, su preparación, su ejecución y sus implicaciones al momento de determinar las autoridades competentes para investigar su cometimiento y juzgarlos.

C) En el primer capítulo la estudiante realiza una introducción al fenómeno de la delincuencia informática. Nos aclara aquellos conceptos relevantes para entender esta forma de criminalidad tales como "hacker", "cracker", "delito informático", "delito computacional", entre otros. De esta forma, permite al lector mantener una lectura mucho más comprensiva y adecuada el contenido de su investigación. Las definiciones aportadas provienen de bibliografía especializada en la materia y se encuentra a lo largo de la investigación estadísticas enfocadas al tema de estudio.

D) La estudiante hace un análisis correcto de la naturaleza jurídica del delito informático así como de los sujetos que intervienen en esta clase de ilícitos penales y el bien jurídico que se trata de proteger a través de la legislación penal y nos introduce al estudio de la "libertad informática" que, desde mi punto de vista, requirió un poco más de tratamiento en la investigación.

E) En el segundo capítulo la estudiante realiza un amplio análisis y enumeración de las normas jurídicas de nuestro ordenamiento aplicables a su tema de estudio. Se parte desde la Constitución justificando la protección jurídica de nuestro derecho al acceso universal a las tecnologías de información y comunicación y el derecho a la intimidad familiar y personal.

Recibido 19/05/2017

F) Continúa su disertación detallando las normas de tratados internacionales y de carácter nacional aplicables, de entre las que se debe destacar las disposiciones de la "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" y el "Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación" y por supuesto, el Código Orgánico Integral Penal, en el que se detiene para analizar las infracciones informáticas en base al criterio de "delitos informáticos como medio" y "delitos informáticos como fin" que es una clasificación interesante aportada por la estudiante.

G) Al realizar un análisis general de las infracciones penales contenidas en el COIP, lamentablemente se deja a un lado la posibilidad de orientar su estudio en un tipo penal en específico o en una clase de delitos informáticos en particular. Considero que la estudiante debería considerar limitar su ámbito de estudio mucho más en una próxima investigación.

H) Se investiga también en la disertación, un tema muy debatido como la jurisdicción en "territorio digital" como lo ha llamado la estudiante. Quizás debió ser un tema de más amplio estudio; sin embargo, los elementos aportados son suficientes, al igual que la determinación de los sujetos procesales y los sujetos auxiliares que intervienen al momento de determinar las infracciones penales informáticas.

I) El capítulo final de la disertación refiere casuística de gran interés en el ámbito nacional e internacional. Es de conocimiento generalizado lo ocurrido con WikiLeaks y por supuesto el caso de Fernando Villavicencio relacionado a la difusión de información confidencial. Considero que se realiza un resumen adecuado de los casos y un análisis comparativo de gran relevancia y directamente vinculado el tema de disertación.

J) Me parece que la estudiante debió extenderse un poco más en el análisis del denominado "hacker" como sujeto activo de un delito informático. Siendo este el tema de su disertación me parece que olvidó explorar un poco más los factores criminológicos del delincuente y su participación en las infracciones penales, lo que implica también estudiar al autor mediato, inmediato y coautor así como la figura del cómplice.

K) Por todas las consideraciones expuestas, califico con **9 sobre 10** la disertación de abogacía cuyo análisis, lectura e informe se me ha encomendado.

Atentamente,

Eduardo León Micheli
Profesor Informante

Quito, 24 de mayo del 2017

Señor doctor,

Iñigo Salvador Crespo

Decano de la Facultad de Jurisprudencia

Pontificia Universidad Católica del Ecuador

Señor doctor

Gonzalo Vaca Dueñas

Secretario Abogado de la Facultad de Jurisprudencia

Pontificia Universidad Católica del Ecuador

En contestación al oficio No. 031-SJG-2017, de 22 de mayo del 2017, a través de la cual me corrió traslado con la designación de Profesor Informante de la disertación de abogacía titulada "EL HACKER COMO SUJETO ACTIVO DEL DELITO, LIMITES Y EXCEPCIONES DE LA INTROMISION TECNOLOGICA DE INTERNET A LA LUZ DEL COIP" de la estudiante María Susana Vaca Loaiza me permito presentar mi informe en los siguientes términos:

1. Luego de la revisión del contenido de la disertación, sin duda alguna un tema de investigación de actualidad, de relevancia y discutido día a día en la realidad nacional. En adición es importante recalcar que esta temática es algo poco abarcado por los estudiantes, lo que le da un factor importante a la iniciativa por la presente investigación.

2. Según la forma observamos que la autora ha realizado su investigación iniciando con un primer capítulo que en lo principal abarca una introducción al fenómeno de la delincuencia informática y nos aclara ciertas definiciones importantes como los diferentes tipos de hacker, partiendo de este como el sujeto principal de la presente disertación. De esta manera permite a los lectores, tener una lectura comprensiva y adecuada a lo largo de la investigación.

3. En el segundo capítulo la estudiante realiza un amplio análisis y enumeración de las normas jurídicas de nuestro ordenamiento aplicables a su tema de estudio. Se parte desde la Constitución, donde a mi parecer hizo falta un enfoque Constitucional más amplio donde se profundicen puntos importantes sobre la temática mencionada, donde justifica la protección jurídica de nuestro derecho al acceso universal a las tecnologías de la información y comunicación y al derecho

a la intimidad personal, haciendo hincapié en la libertad de expresión como un factor predominante a lo largo de la investigación.

4. Continúa el trabajo de investigación detallando una a una las normas de tratados internacionales y de carácter nacional aplicables, entre ellas: La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos" y el "Código Orgánico Integral Penal", entre otras normas importantes que detallan puntos importantes sobre la temática en cuestión.

5. Al realizar un amplio análisis, a mi parecer se deja a un lado la posibilidad de direccionar su investigación a un tipo penal en particular o en una clase de delitos informáticos específica. Considero que la estudiante debió haber limitado su investigación a un solo ámbito de estudio, pero puede ser puesto a consideración para para una próxima investigación.

6. El último capítulo de la disertación presenta casuística de gran interés en ámbito nacional e internacional. Se hace un amplio y detallado análisis de lo ocurrido con WikiLeaks y también el conocido periodista Fernando Villavicencio relacionado a la difusión de información confidencial por parte de ambas partes, en esto se realiza un resumen adecuado de los casos y análisis de gran relevancia vinculada directamente el tema de disertación.

6. Me parece pertinente aclarar que la estudiante debió extenderse un poco más en el análisis de la libertad informática basada en la libertad de expresión y siendo estos, el denominado "hacker" como sujeto activo del delito informático.

7. En relación a las citas constantes de la disertación, las mismas cumplen los parámetros de forma y estilo. Por lo todo lo expuesto considero que la calificación de la presente disertación en razón a los errores encontrados corresponde a NUEVE (9) PUNTOS SOBRE DIEZ.

Por la atención que se preste dar a la presente le anticipo mis agradecimientos.

Atentamente,

Ph.D Efrén Guerrero

Profesor Informante

ABSTRACT:

The evolution of technology has allowed to increase the communication channels and therefore this has generated new forms of crime, giving rise to the attainment of new illegal acts. At present many crimes are consumed through electronic means, which we call "Computer Crime". This is a complex issue since it not only includes legal regulations, but also technical knowledge about computer systems.

The present dissertation seeks to identify the limits and exceptions of technological intrusion in the internet network in the light of the Code of Criminal in Ecuador, being the "hacker", active subject of the above mentioned crime, it is important to mention that the subject of Crimes Computer science has already been covered in other countries, while in our country little or nothing has been developed about it. From this it can be inferred that for our legislation to be considered tacitly a crime is necessary to classify and also persue of this work is being an important investigation abou a forgotten topic.

RESUMEN:

La tecnología ha permitido aumentar los canales de comunicación y, por lo tanto, ha generado nuevas formas de delincuencia, dando lugar a la consecución de nuevos actos ilegales. En la actualidad muchos crímenes se consumen a través de medios electrónicos, que llamamos "delito informático". Esta es una cuestión compleja, ya que no sólo incluye reglamentos legales, sino también conocimientos técnicos sobre sistemas informáticos.

La presente disertación busca identificar los límites y excepciones de la intrusión tecnológica en la red de Internet a la luz del Código Penal en Ecuador, siendo el "hacker", sujeto activo del mencionado delito, es importante mencionar que el sujeto De los delitos La informática ya ha sido cubierta en otros países, mientras que en nuestro país poco o nada se ha desarrollado sobre él. De esto se puede inferir que para que nuestra legislación se considere tácitamente es necesario una clasificación y estudio inmediato de toda esta temática.

Agradecimientos:

Al Dr. Cristian Zambrano por dirigir esta disertación, por todo su aporte y consejo incondicional durante este corrido, por ser el catedrático que me inició en la materia penal y por ser un gran guía.

Al P.h.D Efrén Guerrero por toda su paciencia y entrega durante este proceso, por cada consejo y tiempo invertido en mi disertación, por ser un gran docente y un fantástico sub decano de la facultad y preocuparse por los intereses de los estudiantes, mi eterna admiración y gratitud.

A mi querido Nuevo Acuerdo Estudiantil por darme los mejores momentos en mi paso por la facultad, por permitirme presidirlo y generar cambio dentro de la facultad. A mis compañeros de la Asociación Escuela de Derecho por ser parte final de este proceso.

Dedicatoria:

A Dios y mi madre del cielo por haberme dado la oportunidad de haber llegado hasta este punto y fortalecer mi corazón e iluminar mi mente llenándome de coraje, para lograr mis objetivos, además de colocar a las personas correctas que han sido mi soporte y compañía durante mi periodo universitario.

A mi madre Amelia por darme la vida, por todo su apoyo y entrega en cada momento, por sus consejos, sus valores, por ser mi primera maestra y enseñarme la importancia de amar la carrera a la que dedicarás cada día de tu vida, por estar y permanecer en cada momento de mi vida, pero sobre todo gracias por ser luz en mi vida y por todo su amor.

A mi padre Ramón Alejandro por ser mi ejemplo a seguir, por todo su tiempo escuchándome sin decir ni una sola palabra, por ser el motor de arranque en cada una de mis metas y la mano que me levanta cuando he caído, gracias por ser el ejemplo de tenacidad, perseverancia y constancia que lo caracterizan, por el valor de luchar por tus sueños, por ser mi mejor amigo y por todo su amor, hoy ambos nos graduamos de abogados.

A mi hermano Carlos Alejandro por ser mi compañero de retos, por su paciencia y cariño a lo largo de su vida, por cada consejo y abrazo cuando lo he necesitado, por estar en mis triunfos y derrotas, pero sobre todo gracias por ser mi ejemplo de sacrificio, gracias por toda su bondad.

A mis nonos adorados Carlos Alberto y Rosarito por estar desde mi nacimiento y estrenarse como abuelos, por ser impulso, coraje y apoyo incondicional siempre, por sus eternas sonrisas y caricias llenas de amor verdadero, por sus consejos y su tiempo, por su enorme apoyo y ser parte fundamental de este gran paso y de todos los que he dado, esto es por ustedes.

A mis queridos abuelitos Félix y Susana por sus infinitas sonrisas, por festejar mis logros y ayudarme cada día, por ser ejemplo de lucha y sacrificio, por su eterno amor y cariño.

A toda mi familia por creer en mí y ser parte de este logro, por sus consejos y cariño siempre que lo he necesitado. A la familia Liu Sigcho por su cariño y por ser parte fundamental en este camino, en especial Lili y Lin. A la familia Halberstadt Viteri por ser como mi segunda familia, por su afecto y cariño en este camino, a la familia Ojeda por su cariño y apoyarme a lo largo de este proceso.

A la gente que conocí en las aulas de la facultad y hoy puedo considerarlos mis amigos, en especial a Ivannia, María Eugenia, Nicole, Enrique, Lukas, Victor, Jorge, David y Alejandro por estar en cada paso, permanecer y por su amistad verdadera, soy realmente bendecida y agradecida por tener a cada uno de ustedes.

Tabla de Contenidos.:

Introducción:

La generación actual, es parte del avance tecnológico constante basado en las nuevas necesidades de cada individuo, donde las fronteras han ido desapareciendo como factor positivo de la globalización. El uso consuetudinario de las Tecnologías de la Información y Comunicación (TICs) como parte diaria de la sociedad ha creado una nueva manera de interrelacionarnos con el resto del mundo, debido a esto, el contenido de los sistemas informáticos, nos permite hoy procesar y poner a disposición múltiples opciones de información de todo tipo, al alcance de millones de personas que se encuentran conectados al internet.

La evolución de la tecnología ha permitido aumentar las vías de comunicación y por ende esto ha generado nuevas formas de delinquir, dándose apertura a la consecución de nuevos actos ilícitos. En la actualidad muchos delitos se consuman a través de medios electrónicos, a los que los conocemos como "Delitos Informáticos". Esto resulta un tema complejo puesto que no solo comprende normativa legal, sino conocimientos técnicos acerca de los sistemas informáticos.

La presente disertación busca identificar cuáles son los límites y excepciones de la intromisión tecnológica en la red de internet a la luz del Código Integral Penal, siendo el "hacker", sujeto activo del delito antes mencionado, es importante mencionar que el tema de los Delitos Informáticos ya ha sido abarcado en otros países, mientras que en nuestro país poco o nada se ha desarrollado acerca del mismo. De esto se puede inferir

que para que en nuestra legislación un comportamiento sea considerado tácitamente como delito es necesaria su tipificación.

Al ser una nueva figura delictiva, se presenta como uno de los grandes retos, no dejar en la impunidad a los mismos. Tal es el caso, que existe una amplia confusión al momento de la aplicación de la doctrina, entre el Derecho Informático y el Derecho Penal, sabiendo que el último es el que debe buscar las vías necesarias para poder penalizar este tipo de conductas que terminan afectando a los seres humanos.

El método teleológico de Roxin, apegado al Derecho Penal permite el desarrollo adecuado y sistemático de esta disertación para demostrar el objeto de estudio. Esto debido a que este método, vincula la ley penal con la realidad social; el derecho tiene un contenido social y es esa realidad social la que tiene que ser no solo regulada, sino eficazmente entendida y atendida por el derecho para la consecución de sus fines de seguridad jurídica para la convivencia, sobre la base de la protección a los bienes jurídicos de los miembros de la comunidad.

Ante lo expuesto se entiende que al estar en constante evolución debido a la globalización y al ser una generación que es parte diariamente del avance tecnológico, es imperioso realizar un estudio de este tema. El avance tecnológico cada día es más importante y sostenido de los sistemas computacionales. Las más diversas formas del conocimiento humano, es decir, en referencia: a lo científico, lo técnico, lo profesional y en lo personal están siendo incorporadas a sistemas informáticos, las víctimas son vulnerables, ya que no hay un control eficaz para este tipo de conductas ilícitas.

Esta disertación contendrá tres capitulos, en el primero se estudiará marco conceptual y analítico de la intromisión de la red de internet como delito, esto comprenderá el estudio de la historia del fenómeno, conceptualizaciones básicas acerca de delito informático y el "*iter criminis"* del mismo y por ende puntualizar al "hacking" como practica delictiva a través de los cambios situacionales en la sociedad frente a los nuevos peligros procreados en base a las nuevas necesidades de la sociedad.

En el segundo capítulo pretendo llevar a cabo el estudio del marco jurídico y practica judicial en cuanto al "hacking", comenzando con nuestra Carta Magna y con los diferentes tratados internacionales que afiancen o penen este tipo de conductas delictivas, posterior se verificara en el Código Integral Penal, donde se estudiara el tipo

penal autónomo y como se realiza la practica procesal del mismo en el sistema penal ecuatoriano.

Por último, el tercer capítulo y quizás el más importante de esta disertación, es el análisis de dos casos de "hacking" en el Ecuador donde a través de la aplicación del tipo penal correspondiente y el bien jurídico protegido del caso, se verificara los límites y excepciones a la correcta aplicación de la ley en estos delitos y no permitir que se queden en la impunidad. Finalmente, en las conclusiones se abordarán los temas estudiados en la presente tesis demostrando cuales son límites y excepciones actuales con la finalidad de esta tesis es brindar un aporte doctrinario en el país para quienes se hallan interesados en garantizar la punibilidad de estos delitos.

Capítulo 1:

1. Marco conceptual y analítico de la intromisión de la red de internet como delito:

1.1 El Fenómeno del Hacking:

La sociedad de información fundada con la aparición de los ordenadores se caracteriza por prestar un servicio de comunicación que no reconoce fronteras (Aboso Gustavo, 2006, p. 77). Se debe hacer hincapié en la aparición estas tecnologías en determinados ámbitos sociales de la sociedad de aquella época que giraba por la década de los 50 (Guerra, 2009, p. 53), sabiendo que en esta solo se la utilizaba con fines oficinistas, pero fue hasta la década de los 60 donde en Estados Unidos y Alemania se presentaron los primeros casos de abusos en redes informáticas. A partir de estos acontecimientos se comenzaron a formar las bases de la criminalidad informática y se fue creando poco a poco doctrina de la época (Rovira, 2002, pág. 23).

La incidencia de la criminalidad informática hasta llegar a la sociedad de información actual ha aumentado en un porcentaje muy elevado (Rovira, 2002, pág. 33), ya que al ser muy común la impunidad de los mismos, más gente se ve atraída a consumar este tipo de delitos. Tomando en cuenta que a lo largo de los años no se ha dado el seguimiento adecuado desde el ámbito penal, sino solo desde el perfil criminológico, lo que ha generado la ausencia de tipos penales autónomos que se encarguen de terminar estas conductas ilícitas. Además, es importante mencionar que

cuando se le ha dado la importancia para definir criterios acerca de esta rama los resultados no han profundizado lo necesario.

Los primeros estudios encargados de lo que contemplaban en ese entonces los delitos informáticos se llevaron a cabo de los años 70. (Rovira, 2002, pág. 66) Todas estas investigaciones se realizaban en el plano de la delincuencia económica y de la defraudación, ya que en el momento que se dio apertura a esta clase de delitos, los primeros en aparecer fueron y relacionaron al ámbito bancario ya que era considerada una vía más fácil de realizar hurtos. Así inicialmente Tiedemann, consideraba la "criminalidad mediante computación" como una de las formas de criminalidad económica neutrales, es decir, aquellas que surgen en cualquier sistema económico con independencia de la naturaleza del mismo (La criminalidad económica como objeto de investigación, en cuadernos de Política Criminal, 1983, pág. 121). En este caso se puede identificar como se veía reflejado el bien jurídico patrimonial y no el de la intimidad como en realidad debió ser considerado.

La visión de los delitos informáticos se torna cambiante en los 80 cuando a través de las redes sociales de la época, es decir el periódico y la prensa, empezaron a darse elementos relativos a la intromisión ilegal a la red ("hacking") (Amman, 1989, pág. 55) y de virus informáticos. Fueron todos estos anuncios, además de la vulneración en los sistemas de la telecomunicación los que revelaron al público la situación precaria en la que se encontraba el derecho a la intimidad. Con este cimiento y el avance inmediato de la globalización en el campo internacional se formularon conceptualizaciones con propósitos más globales, para que estos tengan aceptación para aplicación alrededor del mundo. Ejemplificando esto Tiedemann quien menciona a la criminalidad informática como "todas las formas de comportamientos ilegales, y del otro lado perjudicial a la sociedad, que se realizan utilizando un ordenador" (Poder Económico y Delito, 1983, pág. 176).

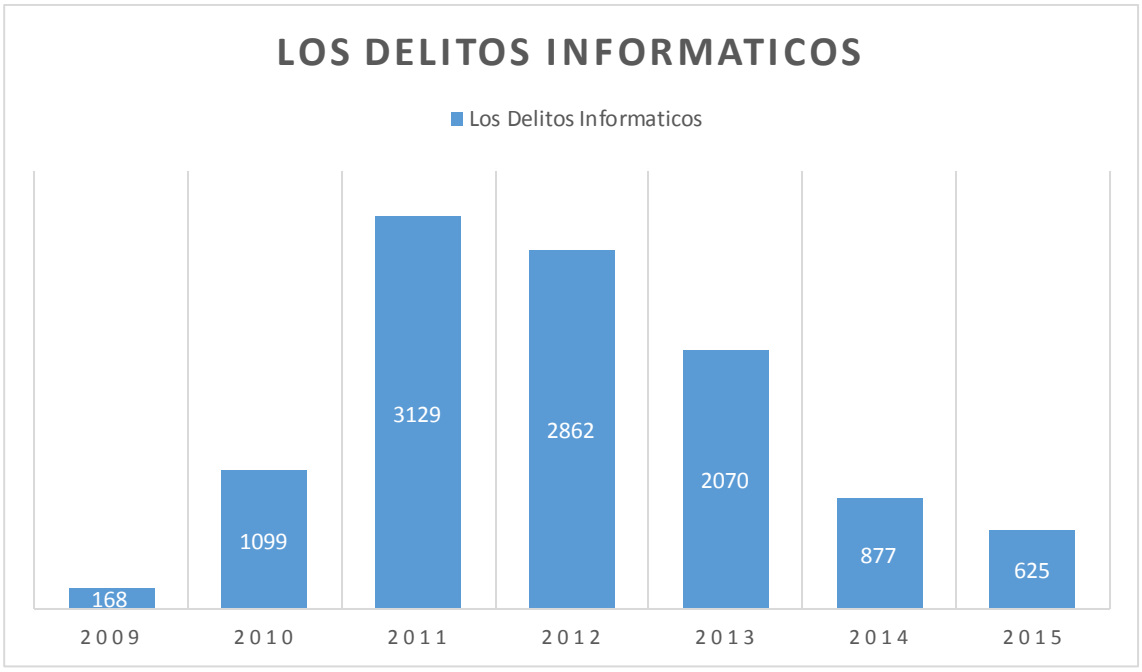
A finales de los ochenta y principio de los noventa los estudios fueron ahondándose los conceptos y generando horizontes más amplios sobre el que ha venido a denominarse como "delitos de datos o información" (Blomm, 1990, pág. 83), figura que actualmente es conocido como delito informático y se le han venido dando diferentes conceptos, pero uno de los más acertados es el de Camacho Losa que menciona lo siguiente:

"Acción dolosa que provoca un prejuicio a personas o entidades, sin que necesariamente conlleve a un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen las actividades informáticas" (Camacho, 1997)

Si bien se menciona muy claro en la definición anterior que realizar este tipo de actividades es una conducta ilícita, la sociedad la ha aceptado como acto consuetudinario que en parte del diario vivir. Lo interesante de los delitos informáticos es que son cometidos en la red de internet y por ende las fronteras estatales no los detienen al momento de la consumación de estos delitos. Es decir, son perpetrados desde cualquier lugar del mundo a cualquier sujeto del mundo que son usuarios de las computadoras, por ello se habla que para darle el control o limites necesarios a este tipo de conductas debería existir univocidad de normativa nacional e internacional referente a la materia. (Aboso Gustavo, 2006, p. 132)

El problema de los delitos informáticos a través del "hacking" aparece debido a que la sociedad no aprovecha este recurso de la manera correcta y abusan de esta para la comisión de actos ilícitos y de satisfacción en contra de otras personas donde estas generan secuelas y nace la interrogante de si el legislador tiene el conocimiento adecuado para no dejar en la impunidad estos delitos y si existen las herramientas y medidas necesarias para que ser utilizados por los antes mencionados. (Aboso Gustavo, 2006)

Haciendo referencia a este fenómeno dentro de nuestro país, en el Ecuador los casos referentes al cibercrimen o también llamados Delitos Informáticos se recibieron en el Ecuador en el año 2015 alrededor de 625 denuncias en diferentes fiscalías del país por delitos cometidos a través de medios informáticos, de las cuales se hablan de apropiación de información en las redes o acoso cibernético a menores de edad o también conocido como "grooming". (El Comercio, 2015)



[1]

Es importante hacer mención que cada día incrementa la comisión de Delitos informáticos en Ecuador. El último estudio realizado a fondo acerca de consecución de estos delitos se realizó en el 2010 por la Unidad de Investigación de Cibercrimen de la Policía Judicial del Ecuador, en este se logró demostrar que estos delitos crecieron en 360% en ese año, generando la duda de cuanto incremento el presente año. (Revelo Hector, 2010, pág. 210).

En el Ecuador existen reportes de la Dirección de Gestión Procesal Penal de la Fiscalía General del Estado donde las cifras son crecientes, sin embargo fragmentan los tipos de delitos informáticos cometidos en el país, donde encontramos: Daños Informáticos al Servicio Privado, Daños informáticos al Sector Público, Apropiación Ilícita por medios electrónicos, Falsificación Electrónica, Suplantación de Identidad por medios informáticos, haciendo un gran hincapié, en la suplantación de identidad a través de las redes sociales con mayor utilización en el país como son: Facebook, Twitter, Instagram, etc. (Estado, pág. 23). Temas que serán tratados a mayor profundidad en el siguiente capítulo.

[1] Tabla de creación propia obtenida del diario El Comercio, "Los servicios de hacker y espionaje se ofertan sin restricción en la web, 2015. Denuncias receptadas en la Fiscalía, desde enero- agosto, entre estas se encuentran violaciones de seguridad a correos electrónicos y robo de contraseñas y tarjetas. (10-10-2016)

1.2El Delito Informático:

1.2.1 Definición de Delito Informático:

El avance de la tecnología ha generado diversas definiciones para este término, sin embargo, no hay una especifico que haya sido escogido por la sociedad para usarlo como único. Varios tratadistas en el tema han hecho un gran acercamiento al tema y han dado un concepto claro y conciso para este término. Entre los más utilizados encontramos las siguientes definiciones.

Calos Sarzana, define el Delito Informático como "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo" (Sarzana, 1999, pág. 123). Nidia Callegari, lo define como "aquel que se da con la ayuda de la informática o de técnicas anexas" (Callegari, 1998, pág. 145). Marìa de la Luz Lima dice en cambio que el famoso "Delito Informático":

"En un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y que, en un sentido estricto y, el Delito Informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya se a como método, medio o fin." (Lima, 2009, pág. 121)

Entre algunas concepciones referentes a este tema, Marìa de los Ángeles Lima me parece una de las más acertadas porque encasilla las diferentes perspectivas de este ilícito como medio, método o fin. Sin embargo, una definición que también me ha llamado la atención y me permitiré citar es, la del doctrinario chileno Renato Jijena Leiva que señala que el Delito Informático es "toda acción típica, antijurídica y culpa, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizada de la misma." (Jijena Leiva, 2006, pág. 121). Esta última definición contiene los elementos de la teoría del delito que permite encasillar correctamente a una conducta como ilícita para no dejarla en la impunidad.

De la misma manera, es prudente desarrollar el planteamiento de algunos autores que en relación con el Derecho Penal mencionan: "Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la

vida social y la jurídica de cada pueblo y cada siglo… (Peso-Navarro, 2001)". Partiendo de esto se busca generar la relevancia que buscar promulgue un acercamiento y genere relación a la normatividad jurídica con la realidad y con las tendencias de la tecnología y los delitos informáticos.

"La especificidad del delito informático le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial" (Choclán-Montalvo, 1997). "La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software" (Davara-Rodríguez, 2007). "Podría ser delito informático todo comportamiento criminal en el que aparezca involucrado un ordenador; de este modo, casi cualquier delito con esta peculiaridad podría ser, eventualmente delito informático" (Aldama-Baquedano, 1993). Todas estas definiciones nos permiten entender de mejor manera cual es el objeto y el fin de la comisión de un delito informático (Ojeda-Pérez, Rincón-Rodríguez, & Arias-Flórez, 2010, págs. 41-66)

El catedrático ecuatoriano en derecho penal informático, Doctor Santiago Acurio del Pino, realiza un aporte extraordinario en esta materia dentro del país, porque al mencionar que sin circunscribir a términos inamovibles como delitos informáticos en su libro hace lugar al término "delincuencia informática", señalando que esto es "todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir o manipular cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera" (Acurio, 2015).

Julio Téllez-Valdés (2007), en su libro de Derecho Informático, nos da una imperiosa puntualización sobre el delito informático desde el punto de vista atípico[2] y lo conceptualiza como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin.

[2] "Entiéndase por atipicidad el fenómeno en virtud del cual un determinado comportamiento humano no se adecua a un tipo legal. La atipicidad a su vez puede ser de carácter absoluto (cuando la conducta examinada no es subsumible en ningún tipo penal) o relativo (por no aparecer alguno o algunos de los elementos de la descripción comportamental)". Obtenido en: (http://jbpenalgeneral.blogspot.com/2011/01/13-atipicidad-de-la-conducta.html 17-01-2017)

Así mismo Acurio en otra de sus publicaciones señala que parte importante de la doctrina menciona "que no estamos frente a nuevos delitos, sino más bien ante una nueva forma o formas de llevar a cabo los delitos tradicionales" (Acurio del Pino S. , 2010, pág. 22). Esta importante aclaración realizada por el catedrático se debe tomar en consideración ya que hace diferenciación entre los delitos tradicionales por medios informáticos, y los delitos de alta tecnología enmarcados como delitos informáticos y encuadrados fuera de los comunes o también llamados tradicionales. El delito informático en sus diferentes tipos debe ser sometido a sanción por el Código Orgánico Integral Penal, siempre y cuando la conducta antijurídica se encuentre tipificada autónomamente y este configurada en su tipo y cuerpo normativo. Es imperioso aclarar que dependiendo de las secuelas que este genere deberá tener un alto índice de reprochabilidad para que no se vuelva a cometer esta conducta (Callegari, 1998).

1.2.1.1 El itercriminis del delito informático:

Los delitos en general son fenómenos psíquico- físicos, ya que estos brotan de la mente del autor y se consuman materialmente a través de la ejecución de una acción o acto determinado que produce la consecución del mismo. Esto es la denominada "iter criminis" (Muñoz Conde, 2003). Esto debido a que inicia desde la idea de querer cometer el delito hasta la consumación del mismo, este se divide en dos fases importantes que son, la interna y externa.

La fase interna está formada por elementos volitivos del fuero interno dela persona y no son punibles (Muñoz Conde, 2003), es decir estos no se encuentran sancionados por el Código Integral Penal, ya que es imposible hacer materia transigible de penar a los pensamientos, pues sabemos que solo se sanciona conductas. En esta fase existen tres momentos diferenciados, siendo estos: la ideación, la deliberación y la decisión.

El primero es el origen de la idea criminal, su mente crea la intención o el deseo de cometer este acto ilícito. La deliberación, es cuando se empieza a desarrollar el plan, apreciando los detalles y las vías o mecanismos a utilizar para la consecución de este delito, además de sopesar cuales son los motivos por los que realiza este delito y valora las secuelas que este dejara. Finalmente, la decisión, es en donde el sujeto decide poner

en práctica todo lo ideado, y dar el paso para la comisión del mismo, ahí concluye la fase interna, sabiendo que esta no es sancionada al encontrarse en el fuero interno de la persona. (Muñoz Conde, 2003)

La fase externa se caracteriza por materializar la voluntad delictiva, va a la consumación del mismo. Es decir, en esta fase el delito cobra vida para ponerse en acción todo el plan desarrollado por el sujeto en la fase interna. En esta fase también existen tres momentos que son los siguientes a mencionar: manifestación de la idea delictiva, los actos preparatorios y la tentativa. (Muñoz Conde, 2003).

Entiéndase al primer punto como la consecución de los actos y acciones que no causan un daño objetivo y se ven reflejados en la determinación de querer cometer el ilícito, este punto no tiene mucha trascendencia jurídica, ya que solamente se manifiesta la voluntad de delinquir, pero mientras no se comete el ilícito no se puede castigar al sujeto. Seguido de esto aparecen los actos preparatorios que se realizan con anterioridad a la ejecución de los delitos que están dirigidos a facilitar la comisión del mismo, sin embargo estos aun no son punibles a menos que estos provoquen en su totalidad la consumación del acto ilícito. (Muñoz Conde, 2003)

Finalmente el "*iter criminis"* cierra su ciclo, con los actos de ejecución, siendo aquellos en el que el sujeto comienza la ejecución del delito independientemente que se termine o no produciendo, es decir que finalmente se consume o quede como tentativa del delito. Esto consiste en la realización de los actos que dan origen propiamente al delito. Los actos de ejecución son punibles en algunas legislaciones, además que se dividen en dos partes importantes como son la tentativa y la consumación. (Muñoz Conde, 2003)

Respecto a los delitos informáticos, el "*itercriminis"* es una figura de interesante investigación debido a su preparación y consumación, debido a que es un delito doloso de acción, que será consumado desde el momento en que el autor pone su voluntad de realizar el tipo, de decidir atentar contra la información, intentando descifrar una clave de acceso, o simplemente poniendo en la red mundial (Internet) una dirección para que pueda ser accedido o hackeado por cualquier persona que está en la red. (Becker, 1990) El resultado es anticipado, ya que este es producido por una acción que constituye el comienzo de la acción típica.

Puede decirse que los delitos de comisión por omisión ingresan en la categoría de delitos informáticos en su mayoría. Por ejemplo, no ingresaría como delito informático el abandono de persona, pero sí la apropiación indebida o la retención indebida. Si bien hay una víctima que no es internet en si mismo, sino siempre una persona, lo cierto es que, para diferenciar, hay que ir al elemento o concepto de bien y de cosa. Se entiende por bien un derecho, y por "cosa" un elemento susceptible de apropiación. Es el caso de todos los elementos que trabajan con energía. Por ello quedarían sin resolverse delitos como el de retención indebida o apropiación indebida, o las violaciones a los derechos de propiedad intelectual, cuando se trata de elementos, "cosas inmateriales" de los cuales pueden existir manipulaciones y generar en consecuencia, víctimas. (Fernandez, 2016)

No se trata de aplicar el derecho penal por analogía, sino el de resolver problemas actuales, puesto que de otro modo se burlaría más del cincuenta por ciento de los delitos previstos y penados en el Código Orgánico Integral Penal. (Fernandez, 2016). En consecuencia, es delito netamente informático, el que involucra que comience y termine en la misma internet, sea con tarjetas de crédito, o apropiaciones como en el caso. Si estamos en presencia de un delito cuyo comienzo es por internet, en el "iter criminis", pero termina fuera del mismo, en un hecho real, es un delito simple. (Fernandez, 2016).

1.2.1.2 Diferencia entre delito informático y delito computacional:

Un conocido catedrático nos menciona que el computador y sus aplicaciones constituyen el objeto material del delito, es ahí donde estamos hablando del Delito Informático, en cambio que si se lo observa como un mero instrumento para la comisión de los actos que generalmente están tipificados en nuestro COIP, ese es un Delito Computacional, es por esto que clarificando la diferencia conceptual entre estos dos tipos de delitos debemos centrarnos y ver la computadora como un medio y un fin para poder diferenciar estas dos acepciones. (Callegari, 1998, pág. 121)

Se entiende que los Delitos Informáticos son actos por los cuales se puede vulnerar o dañar la información y datos como bienes jurídicos protegidos, todo esto se camufla a través de una conducta que contiene los elementos propios que configuran un tipo penal que son: tipicidad, antijuridicidad y culpabilidad. (Araujo, 2014) En cuanto respecta a los Delitos Computacionales podemos decir que son aquellos cometidos por medio o a través del computador empleando las TIC`s (Tecnologías de la Información y

Comunicación) como medio delictivo para la comisión de delitos tradicionales y ya positivizados en el Código Integral Penal.

Para finalizar lo antes expuesto, la diferencia esencial entre las antes mencionadas es que los delitos computacionales usan el computador como fin para poder cometer los delitos que ya se encuentran tipificados en el Código Integral Penal, y los delitos informáticos hacen referencia a la comisión de delitos atentando a la información contenida en medios magnéticos y digitales que son realizados a través de la computadora como un medio.

1.2.2 Delito informático como medio y fin:

El ya citado Téllez Valdés divide a los delitos en dos pautas fundamentales, el uso del "computador" como instrumento o medio, o el computador como fin u objetivo. (Tellez, 1996, pág. 76).

Así, cuando clasifica los delitos como instrumento o medio, nos menciona que estos se considera como tales delitos ya que contienen conductas criminógenas que se valen de la computadora como "método, medio o símbolo en la comisión del ilícito" (Tellez, 1996, pág. 105). Y cuando clasifica la conducta como fin u objetivo, incluye aquellas conductas que se desenvuelven y "van dirigidas contra las computadoras, accesorios o programas como entidades físicas" (Peña, Helen, pág. 3).

Si bien es cierto los delitos informáticos pueden ser enfocados como medios o fin, ya que lo que vale la pena ser rescatado es que la computadora, en sí, puede ser vista desde ambos criterios, esto debido a que puede ser como medio para la consumación del delito, y como fin en relación al objeto material de la infracción, así se podría decir que trabaja el hardware, no sin antes necesitar imperioso e invaluablemente un software. (Fernandez, 2016, pág. 76) .

1.2.3 Naturaleza Jurídica del Delito Informático:

Centrar la naturaleza jurídica del delito informático debe partir de un hecho jurídico, en donde los varios comportamientos irregulares que se dan con el avance tecnológico, determinan algunas conductas que permiten la comisión del delito, debido a esto se vuelve necesario encontrar una forma o método para hacer de estas conductas un hecho

punible y no dejaras en la impunidad como se acostumbra. (Acurio del Pino S. , 2010, pág. 39)

Los Delitos Informáticos en su mayoría son delitos tradicionales que con la ayuda de los Tics suponen nuevas vías de delinquir, que conllevan y en ciertos casos la creación de nuevos tipos penales, y de una nueva tendencia criminal que se conceptualiza y deriva a una nueva manera de aplicar y verificar la validez del principio de territorialidad por la manera en que se cometen estos delitos en cualquier parte del mundo. (Acurio, 2015, pág. 49)

1.2.4 Sujetos del delito informático:

La ejecución de una conducta punible supone la existencia de dos sujetos, se entiende a esto, un sujeto activo y otro pasivo. Estos pueden ser una o varias personas naturales o jurídica y claramente el bien jurídico protegido será definitivamente el elemento localizador de los sujetos y de su posición frente al delito. Siendo el titular del bien jurídico lesionado será el sujeto pasivo, quien puede prorrogar del sujeto perjudicado, el cual, en algunos casos especiales, ser un tercero en cuestión. Es por ello que, en la otra parte, quien lesione el bien que se busca sea protegido a través del tipo penal autónomo, será el ofensor o el sujeto activo. (Libano Manzur)

Es curioso e interesante manifestar que no existe un perfil exacto sobre los delincuentes informáticos. Sin embargo, se habla mucho de características especiales que la sociedad en base a la costumbre ha ido generando como ideas acerca de personas solitarias, orientadas por la tecnología y sus avances, inestabilidad emocional y además conflictos para limitar sus actuaciones y las repercusiones que estas puedan tener ya que solo necesitan una motivación, una creencia racionalizada y obviamente el medio tecnológico de la mano de un momento específico para actuar. (Acurio, 2015, pág. 59)

Claudio Líbano nos menciona que el acceso no autorizado o indebido a los sistemas informáticos es denominado como “hacking”. (Libano Manzur, pág. 66). Se puede entender que el sujeto activo en esta clase de infracciones puede ser cualquier persona, pero para este autor en particular se ha tratado de proponer para esta clase de infractores un calificado denominado “Pirata Informático” (Hacker o Crackers), a mi parecer esta manera de visualizar este campo termina siendo muy limitante y focalizada, se entiende esto debido a que existen ciertas personas sin las características mencionadas que por

motivos laborales, se dedican a estas actividades y no lo hacen por el mero hecho de ser piratas en red.

1.2.4.1 El delincuente informático:

El perfil del delincuente informático tiene ciertas cuestiones que le permiten cometer el ilícito, estas características son del todo técnicas, donde el elemento volitivo y cognitivo buscan hacer un daño sobre un bien jurídico protegido con el objetivo de destruirlo, alterarlo o divulgar la información deseada respecto al antes mencionado bien.

A pesar de que la sociedad se encuentra en constante evolución, resulta un verdadero desafío extraer al "hacker" del imaginario social en el que la humanidad lo ha venido posicionando con el paso de los años y que ha sido considerado de manera equivocada por el derecho penal. En este sentido fue considerado como el único sujeto cuando la doctrina habla respecto a cibercriminalidad; esto se dio debido a que el primer participe directo en la comisión de los ilícitos fue el "hacker" centrado a la intromisión en sistemas informáticos, que reducen el modelo de "un genio informático, superdotado y con problemas de adaptación sociales tales que llevan a volcar todo su interés en un universo cibernético" (Muñoz., 2006, pág. 19). Respecto a esto la nueva era de la tecnología y la sociedad cambiante nos precisa que no se puede identificar al hacker con el criminal de los delitos informáticos,[3] sino hay múltiples escenarios, ya que no existe un solo perfil del criminal de delitos informáticos.

Al hablar del delincuente informático se hace referencia a cualquier sujeto que delinque y usa como medio el ciberespacio como parte esencial o central del delito, (Mirò, 2012, pág. 230) . La idea de la multiplicidad de los perfiles del delincuente informático es totalmente coherente con la clasificación de los delitos informáticos es completamente coherente ya que una parte importante para la consecución el ilícito es la base del propósito del delito informático, entre crimines políticos, económicos o sociales.

1.2.4.2 Sujeto Activo:

[3] Pinguelo, F. "Virtual Crimes, Real Damages" Dice expresamente, op cit, p.121 "No existe un perfil estático del ciberdelincuente, ya que estos adquieren distintas formas en su intento de robar, engañar o destruir"

En el ámbito penal se entiende que el sujeto activo es "aquella persona que realiza la acción penal u omite la acción penal esperada, que en algunos casos la ley exige una condición específica" (Zambrano, 2014).

En el área de los delitos informáticos si se habla del sujeto activo, es el sujeto conocido por la sociedad como "hacker", aquel individuo con características especiales al tener una habilidad con el manejo de los sistemas informáticos, y que en algunos casos por su situación laboral se encuentra en posiciones estratégicas donde manejan información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando en muchos de los casos no realicen actividades laborales que les den la apertura necesaria para la comisión de estos ilícitos. (Levene, 2006).

Al entablar al hacking desde una posición laboral, cargo o rol dentro de una empresa y su manejo de información para cometer estos actos ilícitos actuando desde una empresa, negocio, organización u otro se los denominara INSIDERS, y los que teniendo conocimientos profundos en cuanto a los sistemas informáticos y que cometen estos ilícitos siendo agentes externos a las empresas, negocios u otros, se los denominara OUTSIDERS. (Levene, 2006)

En general el conflicto radica en lo relacionado al sujeto activo como ente principal para la comisión de este ilícito informático, radica en el hecho que la mayoría de ilícitos son cometidos por los llamados INSIDERS, debido a que por estos se facilita la comisión del delito y se da paso a utilizar información que no les pertenece y afectando principalmente al dato como bien jurídico tutelado por el Estado.

El nivel típico de aptitudes que posee un delincuente informático es un tema coyuntural ya que para algunas personas el nivel de aptitudes no es el indicador oficial para medir el nivel de delincuente informático, mientras que otros señalan que los posibles delincuentes son persona listas, decididas y motivadas aceptar un reto tecnológico, características que pudieran tener en un empleador de procesamiento de datos. (Acurio, 2015, pág. 56)

Al tener claro lo señalado en el párrafo anterior respecto a las características de las personas que cometen delitos informáticos, especialistas en la materia los han catalogado como "delincuentes de cuello blanco" termino introducido por el criminólogo norteamericano Sutherland en 1943. El antes mencionado señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aun sabiendo

que muchas de estas conductas no están tipificadas en algunos ordenamientos jurídicos del mundo, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, e contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, entre otros" (Sutherland, 1943)

El Dr. Acurio menciona en su libro que tanto los delitos informáticos como los delitos de cuello blanco no están de acuerdo al interés protegido como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. (Acurio, 2015, pág. 56). En el caso de los delitos informáticos se crea un síndrome que se hace llamar el de "Robin Hood", es decir:

"La creencia en cierto modo patológica e que mientras que robar a una persona física que tiene sus problemas y necesidades materiales como todo hijo de vecino es un hecho inmoral e imperdonable, robar a una institución como la banca que gana decenas de miles de millones al año es casi un acto social que contribuye a una más justa distribución de riqueza" (Gutierrez, pág. 2)

Respecto a todo lo antes relatado se puede señalar que los Delitos Informáticos no poseen todas las características de los delitos "de cuello blanco", si coinciden en algunas conductas, por tanto, se aclarara que la cualificación del sujeto activo no es un elemento determinante en la delincuencia informática. Solo algunos delitos particulares, como los que son consumados por los hackers propiamente dichos, podrán considerarse como realizados por un sujeto calificado para esta conducta especifica.

1.2.4.3 Sujeto Pasivo:

Se puede decir que el sujeto pasivo o a quien llamaremos a continuación como la víctima, es aquel sujeto o persona sobre la cual recae la acción antijurídica cometida por el sujeto activo a través de la computadora u objeto telemático con la ayuda de las tecnologías de la información o TIC`s.

Tomando en cuenta presta atención en algunos casos la víctima del delito informático es la persona que tiene conocimientos nulos o escasos sobre informáticos porque sobrelleva su vida en un plano de normalidad no asociada a los sistemas de información, por lo cual, por dicho desconocimiento se vuelve presa fácil o vulnerable los llamados ciberdelincuentes que en la actualidad tienden a atacar a su objetivo después de analizar todas las habilidades. (Acurio, 2015)

1.2.5 Clasificación de los Hackers:

Si bien es cierto que se afirmó que el cibercriminal no puede identificarse solamente con los hackers, tampoco existe un solo tipo de hacker, ya que existen algunas clasificaciones para este en base a sus diferentes expectativas a la hora de entrometerse en los sistemas informáticos. (Mirò, 2012, págs. 231-232) El hacker es un sujeto que ha ido evolucionando en base a las necesidades de la sociedad, desde los *true hackers*, personas aficionadas a la informática en los primeros días de la aparición de esta tecnología en los años sesenta, pasando a los crackers de los años noventa que incluye a quienes usan las redes de información para acceder ilícitamente a los sistemas informáticos. (Mirò, 2012, págs. 232-233).

Lo que se persigue en la actualidad es analizar los diferentes tipos de personas que participan en la criminalidad y en este tipo de conductas ilícitas en el ciberespacio, comenzando por el análisis de las figuras generalmente asociadas a este tipo de conductas, como son las de "hackers y crackers", y tratando después de individualizarlo a categorías para poder contrarrestar esta clase de actos, teniendo en cuenta casos similares en la actualidad para encontrar soluciones similares y aplicables casos futuros.

Siendo así categorizaremos a los sujetos del hacking de la siguiente manera:

a) **Hacker:** Aquella persona o sujeto que hace del hacking un arte, descubriendo para generar soluciones tecnológicas que puedan ayudar o beneficiar a un grupo focalizado de la sociedad. (Acurio, 2015, pág. 42) De los hackers más conocidos en la sociedad están Jay Freeman alias" Saurik" (Creador de Cydia para dispositivos Apple), Bill Gates (CEO de Microsoft) y Marck Zuckerberg (Creador de Facebook) (Acurio, 2015, pág. 42)

b) **Cracker:** Es aquella persona dedicada a modificar, alterar o suprimir características esenciales de un programa informático con un fin malicioso o en algunos casos pecuniario. De los casos más comunes que se dan en el área económica, se basa en que el cracker modifique con un fin malicioso en los cuales los crackers modifican el código fuente del programa sin que tener que

pagar a licencia de este. Entre los programas crackeados con frecuencia están los antivirus o las licencias operativas de Windows. (Acurio, 2015, pág. 42)

c) **Black Hat**: Los así llamados o también conocidos como hackers de sombrero negro, son aquellos que se encargan de violar la seguridad de los sitios de internet, aplicaciones, bases de datos y sistemas automatizados de información con fines maliciosos, que esperan a través de esto fines pecuniarios como su vía de ganarse la vida. (Zwicky, 2010, pág. 487)

   Los Black Hat Hackers o Hackers de Sombrero Negro son los chicos malos, los que comúnmente se les refiere como simples Hackers. El termino se usa mucho específicamente para los Hackers que rompen la seguridad de una Computadora, un Network o crean Virus de Computadora.

   Los Black Hat Hackers continuamente buscan la forma de entrar o romper la seguridad de lo que quieren, haciéndole la vida más difícil a los White Hat Hackers. Los Black Hat Hackers a menudo buscan el camino de menor resistencia, ya sea por alguna vulnerabilidad, error humano, vagancia o algún nuevo método de ataque. La motivación número uno de un Black Hat Hackers es el dinero. La clasificación de Sombrero Negro proviene de la identificación de los villanos en las películas antiguas del viejo oeste que típicamente usaban Sombreros Negros. (Miguel, 2016)

d) **White Hat:** Estos son los conocidos hackers de sombrero blanco que se encargan de crear sistemas informáticos y programas con el propósito de beneficiar a un grupo focalizado de la sociedad, además se encargan de explotar fallas y vulnerabilidades de sistemas informáticas con el fin de recomendarse y dar todas las sugerencias pertinentes para la protección en teas de seguridad de la información. (Zwicky, 2010, pág. 487)

   Los White Hat Hackers o Hackers de Sombrero Blanco son los chicos buenos, los éticos. Regularmente son los que penetran la seguridad de sistemas para encontrar vulnerabilidades. Algunos son consultores de seguridad, trabajan para alguna compañía en el área de seguridad informática protegiendo los sistemas de los Black Hat Hackers. Es importante mencionar que algunos fueron Black Hats y brincaron al bando de los buenos o tienen los conocimientos de ellos y los utilizan para hacer el bien. (Miguel, 2016)

e) **Gray Hat:** Un hacker de sombrero gris, este sujeto es un hibrido del hacker de sombrero negro y sombrero blanco, que algunas veces actúa de manera ética informando sobre ciertas vulnerabilidades y otras veces explota estas de una manera antiética para beneficio propio. (Zwicky, 2010, pág. 487)

Los Gray Hat Hackers o Hackers de Sombrero Gris son los que juegan a ser los buenos y los malos, en otras palabras, tienen ética ambigua. Tienen los conocimientos de un Black Hat Hacker y los utilizan para penetrar en sistemas y buscar vulnerabilidades para luego ofrecer sus servicios para repararlos bajo contrato. (Resa, 2005, pág. 121)

1.2.6 Factor Criminógeno y tipología de los Delitos Informáticos:

1.2.6.1 Factor Criminógeno:

Existen diferentes tipos de delitos informáticos, sin embargo, resulta bastante oportuno reconocer que todos estos delitos poseen un factor criminógeno que genera lo proliferación de este tipo de conductas. Los sistemas informáticos y todas las aplicaciones que rodean a este antes mencionado, brindan grandes posibilidades de cometer actos ilícitos punibles o actos que tengan alguna clase de consecuencia jurídica, lo que genera como resultado un procesamiento de datos con un alto factor criminógeno, es importante mencionar que uno de los grandes factores que genera la consecución de estas es la información brindada por los usuarios de este servicio al colocar diferente tipo de información personal en los sistemas telemáticos.

La proliferación de delitos informáticos tiene tres factores importantes que son: el desconocimiento de los nuevos sistemas de información, la inexistencia de precariedad de los sistemas de seguridad y la falta de leyes y normativas especiales para esta clase de conductas. (Rovira, 2002) El desconocimiento de los nuevos sistemas de tratamiento de información tiene como protagonista al usuario del sistema informático, donde cada vez existen más y jamás contemplaron la idea de lo que podía suscitarse al manejar incorrectamente un computador. (Acurio, 2015, pág. 51) La sociedad crea sus propios riesgos dentro de los sistemas de información basada en las necesidades diarias de ingresar a los sistemas informáticos y también existe el deseo de crear sistemas de seguridad que de alguna manera protejan la

información que genera una persona dentro de estos sistemas ya que esta se encuentra al alcance de todos y puede ser utilizada con fines diferentes.

Otro factor mencionado por Rovira, es la inexistencia de sistemas de seguridad y en el caso de su existencia tiene muy poca eficacia y sus niveles de efectividad son muy bajos. Esto se basa en el desconocimiento de los riesgos existentes que genera la incorrecta utilización del computador. La información que posee un sistema informático en algunos casos puede ser de carácter público, mientras que en otro deberían existir factores de seguridad mínimos para precautelar la privacidad de los usuarios y al ser de continuo avance los sistemas tecnológicos, la seguridad resultaban precarios. En tal caso es necesario que se asuma una conducta cambiante dispuesta a generar diferentes sistemas que se acoplen a las necesidades del momento para que exista un sentimiento de seguridad por parte de los usuarios.

El último factor y quizás el más importante se ve enfocado en la inexistencia de normativa especial que otorgue la suficiente capacidad a los gestores de justicia para poder argumentar sus decisiones referentes a este tipo de ilícitos, puesto que la inexistencia de los mismos ha generado una brecha entre las autoridades y la sociedad ya que su atribución para combatir estos ilícitos no cuenta con un sistema tipificado que le permita hacerlo. Según lo menciona Acurio, algunos países del mundo consideraron poco necesario la creación de leyes para esto ya que consideraban que estas conductas se podían subsumir a los delitos tradicionales. (Acurio, 2015, pág. 53)

El delito informático al ser una figura no tradicional presenta un verdadero atractivo para quienes desean realizarlo, son algunas las razones por las que este llama la atención de muchos usurarios dentro los sistemas de información (Borghello, 2009), entre estos están:

a. Dependencia de la tecnología.
b. Anonimato y Suplantación de Identidad.
c. Facilidad de Adaptación.
d. Escalabilidad.
e. Universalidad de acceso.
f. Proliferación de herramientas y códigos.
g. Dificultad para encontrar a los culpables.

h. Intangibilidad de las pruebas.
i. Grupos de Delincuentes Profesionales.
j. Escasa consciencia por parte del usuario.

Todos estos factores son de alto interés para quienes consideran la comisión de los ilícitos, la relación o vinculación que se genera con y para la tecnología hace que los usuarios se vuelvan dependientes de esta, consecutivamente al volverse dependientes de la misma la gran facilidad que se presenta ara "desaparecer" en el mundo virtual dificulta conocer a la persona que causo el daño y resulta algunas veces imposible el rastreo de los responsables de este ilícito. (Acurio, 2015). Las herramientas de los sistemas informáticos pueden ser fácilmente modificadas y permiten que estas personas se adapten al medio para cometer estos ilícitos, sabiendo que un solo cambio al sistema informático puede causar grandes daños en futuros ingresos.

Cualquier persona del mundo que sea participe de los medios informáticos puede volverse un "delincuente informático", ya que las herramientas están al alcance de toda la sociedad, es decir de sujetos activos y pasivos de la conducta informática punible. Una cuestión interesante es que además de encontrarse al alcance de todos nosotros, las propias páginas de internet nos ofrecen tutoriales de como volverse un sujetos activo en esta acción ilícita, otro factor que es predominante para quienes se interesan en la comisión de esto versa sobre la dificultad de establecer caminos legales para llegar al delincuente debido que para este no existen fronteras y las jurisdicciones internacionales a un no han encontrado la vía adecuada para controlar esto. (Castells, 2001).

No solo resulta un gran inconveniente para las autoridades el lugar de la comisión de los ilícitos sino también la capacidad de encontrar pruebas válidas para que sean aceptadas por los tribunales al momento de juzgar este tipo de conductas ya que, en algunos casos son realizados por grupos integrados por distintas personas con diversos niveles de conocimientos, pueden ser: técnicos, legales y financieros que logran que de alguna manera sea un delito perfeccionado lo que genera la intangibilidad de la prueba para la utilización de estas en las cortes. Finalmente, otra cuestión importante es que no existe la cultura necesaria de los usuarios del internet, ya que poseen herramientas de seguridad, pero no tienen capacitación para su debida utilización y sean de ayuda para los gestores de justicia para que de alguna manera frene las conductas ilícitas. (Acurio, 2015, pág. 55)

1.2.6.2 Bien Jurídico de los Delitos Informáticos:

A lo largo de la carrera de derecho sabemos que el bien u objeto jurídico es aquel que algún caso es puesto en peligro o se ve lesionado por lo que los gestores de justicia se ven en la obligación de reparar esto o garantizar que este no se vea lesionado. (Araujo, 2014). Dentro de lo que respecta los delitos informáticos, al ser una figura nueva se trata de proteger a los bienes jurídicos a través de los delitos tradicionales (Acurio, 2015, pág. 84), con una nueva interpretación teleológica como menciona Roxin para resolver las lagunas originadas por estos interesantes nuevos tipos penales.

Sin embargo, existen otras vertientes doctrinarias que observan estas figuras desde otro punto de vista, que menciona a la sociedad de la información hace necesaria la aparición de bienes intangibles, puesto que varios delitos informáticos se caracterizan por este. Los bienes jurídicos de protección que son los que se ven tutelados según esta nueva vertiente toma en cuenta los bienes tangibles e intangibles. La cuestión radica que la intangibilidad de los bienes no está constitucionalmente protegido es por eso que en base a los tangibles se busca una conexión existente para conectarlo y volverlo un bien jurídico protegido.

Es decir, se entiende que la protección de la información debe tener como bien protegido cualquier actividad que genere daño a la persona por utilización de esta. (Fernandez, 2016, pág. 56). Sin embargo, si buscamos puntualizar el bien jurídico protegido por la utilización de sistemas informáticos es la llamada "libertad informática" (Acurio, 2015, pág. 86) esta se ve encaminada como cierta figura de expresión que genera libertad en el individuo de utilizar los sistemas de información o las computadoras en base a los límites constitucionales. Es por esto que se entiende que los delitos informáticos es la violación a la libertad de los usuarios a la utilización de las redes como el internet, entre otras. Estos usuarios que son parte de la sociedad de información además de poseer libertad en la utilización de los medios informáticos también se ven vinculados a los bienes jurídicos protegidos tradicionales para la efectividad de las medidas existentes por parte del legislador, tales pueden ser:

a. El patrimonio.
b. La reserva, la intimidad y confidencialidad de los datos.
c. La seguridad o fiabilidad del trafico jurídico o probatorio.
d. El derecho de propiedad.

El bien jurídico protegido acoge varios factores del ser humano como son la confidencialidad, integridad disponibilidad de información donde esta se almacena o se transfiere. (Acurio del Pino, 2010, pág. 97). Frente a esto se entiende que los delitos informáticos no atacan a un solo bien jurídico, sino a la cantidad de varias conductas que subsumen al acto ilícito a través de los sistemas informáticos.

1.2.6.3 Tipología de los delitos informáticos:

La clasificación de los delitos informáticos es amplia, existe mucha diversidad acerca de las conductas ilícitas que terminan afectando a la sociedad. Sin embargo, Camacho Losa nos habla de tres factores que configuran el límite de la clasificación de los ilícitos que giran en torno a: la imaginación del autor, su capacidad técnica y las deficiencias del control existentes en las instalaciones informáticas. (Acurio, 2015, pág. 89). Es importante rescatar que existen innumerables conductas ilícitas que rodean los delitos informáticos, sin embargo, rescatar un número exacto le permite al legislador buscar mecanismos que subsanen estas conductas directamente para no dejar en la impunidad este tipo de delitos, siendo algunos de los delitos informáticos:

1. Los fraudes:
    - 1.1 Los datos falsos engañosos.
    - 1.2 Manipulación de programas.
    - 1.3 Técnicas de salami.
    - 1.4 Falsificaciones Informáticas.
    - 1.5 Manipulación de datos de salida.
    - 1.6 Clonación de tarjetas de crédito.
    - 1.7 Clonación de tarjetas de débito.
    - 1.8 Pishing.
2. Sabotaje informático:
    - 2.1 Bombas lógicas.
    - 2.2 Gusano informático.
    - 2.3 Virus informático y malware.

2.4 Ciberterrorismo

2.5 Ataques de denegación de servicio.

2.6 Las redes robot.

3. El espionaje informático y robo o hurto de software.

3.1 Fuga de datos.

3.2 Reproducción no autorizada de programas informáticos.

4. El robo de servicios:

4.1 Hurto de tiempo del computador.

4.2 Apropiación de informaciones residuales.

4.3 Parásitos informáticos.

5. Acceso no autorizado a sistemas informáticos:

5.1 Las puertas falsas.

5.2 La llave maestra.

5.3 Pinchado de líneas.

5.4 Piratas Informáticos. (Acurio, Derecho Penal Informatico, 2015)

Capítulo 2:

2. Marco Jurídico y practica judicial conforme al "Hacking"

2.1 Marco Jurídico Ecuatoriano:

En Ecuador se ha generado gran temor y conmoción que han causado incertidumbre en la sociedad de información ecuatoriana (Jara, 2015), todo esto debido a que los sistemas electrónicos se han vuelto un blanco para cometer diferentes actos ilícitos, tales pueden ser: extorción, robo, fraude, suplantación de identidad entre algunos otros que se han venido desarrollando con el avance de la tecnología. Esta nueva tendencia de la delincuencia informática, resulta una tarea comprometida y de difícil entendimiento lo que conlleva a la dificultad de una conceptualización plena del mismo, se entendería que estas conductas deben estar regladas por la legislación

ecuatoriana y se tome a consideración la utilización de tecnologías para la comisión del delito.

Las cifras de los delitos informáticos cometidos en el Ecuador resultan un poco inciertas, debido a que las pocas denuncias que se realizan, ya sea esto por falta de conocimiento o interés que deja un vacío legal enorme (Balseca, 2016), lo que deja en la impunidad muchos de los cometimientos de esta índole. Esto dentro de lo que comprende un marco legislativo termina siendo un reto particular para verificar la eficacia de la legislación actual referente a este tipo de delitos.

Dentro del desarrollo de mecanismos que garanticen la eficacia de la correcta utilización de los medios informáticos, el Ecuador ha buscado la manera de contrarrestar la impunidad de estas conductas tipificándolas en ciertas leyes.[4]

Cabe mencionar las leyes, reglamentos, decretos y resoluciones que engloban el marco normativo ecuatoriano y buscan precautelar al usuario en defensa de sus derechos cuando estos se han venido vulnerando, por la incorrecta utilización de los sistemas informáticos.

Sin embargo, en la presente disertación se mencionarán las normas más importantes, que sirven para el desarrollo adecuado de la misma y se adapten a la realidad actual ecuatoriana, como la reciente publicación del Código Orgánico de la

[4] El régimen jurídico del delito informático a diferencia de otras figuras de nuestra legislación se encuentra contenido en varios cuerpos legales dispersos, sin embargo, el artículo 17 del Código Orgánico Integral Penal señala que las solo las conductas tipificadas en el código son punibles, a pesar de esto, dentro de estos cuerpos legales existe información importante en relación a los delitos informáticos, siendo estos:

1. Constitución de la República del Ecuador.
2. Código Orgánico Integral Penal.
3. Código Civil Ecuatoriano
4. Código de Procedimiento Civil.
5. Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación
6. Ley Orgánica de Transparencia y Acceso a la información pública.
7. Ley de Protección de los datos.
8. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
9. Ley de protección de usuarios del sistema financiero
10. Decreto Ejecutivo No. 1014 sobre "El uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador"
11. Resolución SBS JB-2011-1923 "Controles en los Cajeros Automáticos"
12. Ley Orgánica de Comunicación.

Economía Social de los Conocimientos, Creatividad e Innovación donde, se habla mucho del acceso al internet o la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su correcta aplicación enmarcado en la Constitución y el Código Orgánico Integral Penal que se encarga de sancionar este tipo de conductas.

2.1.1 Constitución de la República del Ecuador:

Si bien es cierto que la Constitución de la República del Ecuador directamente sobre los delitos informáticos dentro de la carta magna de la nación, se hace mención a ciertos bienes jurídicos protegidos que son parte de este tipo de conductas.

1.Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:

2. - El acceso universal a las tecnologías de información y comunicación.[5]

2. Art. 66.- Se reconoce y garantizará a las personas:

20. El derecho a la intimidad personal y familiar.[6]

El artículo 16 el acceso universal a las tecnologías de información y comunicación, lo que le da apertura a la sociedad a ser partícipes de la red de internet, lo que genera la consumación de delitos informáticos por parte de personas que buscan causar daño a otro sujeto.

El articulo 66 nos garantiza el derecho a la intimidad lo que se ve completamente comprometido al ser violentado con la comisión de delitos informáticos, puesto que la intromisión a la red de internet, causa el acceso a información de carácter privado y personal. Tomando en cuenta la existencia de esta norma, es importante mencionar que al dar la apertura a la tecnología a la información y al proteger el derecho a la intimidad, deberían existir mecanismos eficaces que garanticen la eficacia de este derecho y no generen la impunidad en varios de estos delitos.

2.1.2 Tratados Internacionales:

Dentro del marco jurídico internacional cabe recalcar a la Organización de Estados Americanos, organización a la cual Ecuador forma parte (OEA, 2016), que al dar

[5] Oficial, R. (2008). Constitución de la República del Ecuador. *publicado en el Registro Oficial de octubre, Ecuador*.
[6] Oficial, R. (2008). Constitución de la República del Ecuador. *publicado en el Registro Oficial de octubre, Ecuador*.

ejecución a las conclusiones y recomendaciones de las Reuniones de Ministros de Justicia (REMJA), así como de las recomendaciones de su Grupo de Trabajo en Delito Cibernético, la Secretaría Técnica de la OEA, mencionan que cada país dentro de su legislación nacional debe tener algún tipo de normativa que regule este tipo de conductas. (OEA, 2016)

Otro tipo de tratados que se toman en consideración para el manejo de este tipo de conductas y nuestro país ha ratificado son:

a. El convenio de Berna, que fue ratificado en nuestro país por la Ley 22195 ratificado el 09 de octubre de 1991.[7]
b. La Convención para la Protección y Producción de Phonogramas de 1971 ratificado el 04 de junio de 1974.[8]

Es imperioso mencionar que, en los años 80, la Organización de Cooperación y Desarrollo Económico (OCDE), fomento el estudio de la posibilidad de aplicar de manera internacional normas de carácter penal que busquen perseguir la justicia y no dejar en la impunidad los delitos informáticos por el uso indebido de los sistemas informáticos. Hay que tomar en cuenta que las posibles vías económicas de la delincuencia informática, tienden a un carácter internacional e incluso no ve fronteras para la comisión del delito. (OEA, 2016)

En el año 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en todos los estados partes y en esta se recomendaba ciertas medidas para contrarrestar este tipo de conductas ilícitas en sistemas informáticos. (OEA, 2016).

La Organización de las Naciones Unidas en el año 1990 en el "Congreso sobre prevención del Delito y Justicia Penal" celebrado en Cuba, se menciona que la delincuencia informática avanzó drásticamente con el aumento de empleos en procesos de datos y manejo de la economía de los diferentes países del mundo. Tal es el caso que

[7] El estado ecuatoriano se adhirió al Convenio de Berna el 08 de julio de 1991, sin embargo, este entro en vigor 09 de octubre de 1991. Acceso en: http://www.wipo.int/treaties/es/remarks.jsp?cnty_id=945C (26-01-2017)

[8] El estado ecuatoriano se adhirió a la convención para la protección y producción de fonogramas en el 29 de octubre de 1971, pero ratifico el 04 de junio de 1974 y entro en vigor el 14 de septiembre de 1974 Acceso en: http://www.wipo.int/treaties/es/remarks.jsp?cnty_id=945C (26-01-2017)

la ONU, ha publicado una propia descripción de los "Tipos de Delitos Informáticos" en la cual buscó frenar la aparición de estos delitos o en su defecto la propagación del mismo. (ONU, 1990)

El desarrollo de las tecnologías ofrece una visión negativa, ya que ha dado apertura a la comisión de conductas antisociales y delictivas. Los sistemas informáticos a más de ofrecer oportunidades nuevas a la sociedad, también nos genera vías para infringir la ley de manera anónima o desde cualquier parte del mundo, ya que los delitos informáticos al no ser tradicionales, una de sus peculiaridades que no tienen fronteras. Por esto los organismos internacionales alrededor del mundo, realizan esfuerzos para viabilizar mecanismos y proyectos que en coordinación de los estados nacionales pueden materializarse en un periodo corto (Bejarano, 2015)

2.1.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Respecto a esta ley, es importante mencionar que de alguna manera fue el primer acercamiento por parte del estado ecuatoriano para encontrar mecanismos suficientes para contrarrestar las conductas ilícitas que estaban causando delitos informáticos en el país. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, que también es conocida por algunos de nosotros como la "Ley 67", esta fue publicada en el Registro Oficial, del suplemento 557 del 17 de abril del año 2002, de alguna manera mediante esta ley se busca castigar los ilícitos informáticos de la Sociedad de Información.

Dentro de las normas estipuladas en este Código se habla de infracciones informáticas, destrucciones maliciosas, entre otras. Todo esto se encuentra abarcado desde el articulo 57 hasta el 64 del presente código, que en la actualidad se encuentran tipificados y regulados el Código Orgánico Integral Penal. [9]Donde para conocimiento

[9] Art.57 Infracciones informáticas. - Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.
Art.59.- Destrucción Maliciosa de Documentos.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

de todos, se redactan los primeros pasos de la legislación ecuatoriana para contrarrestar estas conductas que generan daños a terceros como medio o fin un sistema informático.

En base a esta normativa se entiende que un acto se vuelve punible cuando cumple ciertos elementos probatorios o también conocidos como elementos de convicción. Los elementos de convicción, son el conjunto de pruebas electrónicas necesarias para probar un delito, sin las cuales se entiende la imposibilidad de colocar una pena a este ilícito. En esta normativa se notifica que para que la pericia sea válida

---

Art.60.- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:
1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.
Art.61.- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.
Art.61 últ.inc.- Destrucción de instalaciones para transmisión de datos.- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.
Art.62.- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.
Art.62 últ.inciso.- Pena.- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:
1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes.
Art.63.- Estafa.-Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.
Art.64-, Violación Derecho a la Intimidad.- Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
Obtenido en el R.O/ Sup. 557 – 17-04-2002.

debe ser realizada por personas avaladas por las instituciones del estado para ser avalado como figura probatoria en juicio.

La figura o nueva tendencia que aparece debido a la publicación de esta casusa. La tendencia que se genera pasa a ser llamada "*Actioinformatio per causa"* o también denominada "Accion de información por la causa", esto consiste en que el momento que existe un retraso en una pericia para investigación judicial dentro de un proceso, sin importar que este se encuentre en instrucción fiscal, indagación previa u alguna otra etapa, la parte que se encuentra agraviada puede recurrir a un tercero que es un perito privado para que les brinde su servicio y no quedar en la indefensión. (Aez, 2010, págs. 48-49)

Otro de los puntos de este código que resulta imperioso mencionar es uno de sus grandes objetivos que se centra en precautelar los derechos de los usuarios que hacen negocios en Internet normando la publicidad en línea, fortaleciendo el derecho a la privacidad de los usuarios y otros temas de protección al consumidor en un medio completamente nuevo en el cual es necesario innovar para estar acordes a la tecnología y a los nuevos modelos de negocios y transacciones que se pueden realizar a través de medios informáticos, y evitar que exista intromisión tecnológica a la red de internet por parte de personas que busquen causar daño.

Resumiendo, la aparición de este código fue un paso enorme a la brecha producida por la consecución de delitos informáticos en el país, tal es así que una de las partes importantes recae sobre la apropiación ilícita con la utilización de medios informáticos para facilitar la apropiación de bienes ajenos, valores o derechos, siendo interesante la peculiaridad del caso que la ley agrava la sanción cuando se viola o se rompen claves, criptografía o mandos a distancia. En la estafa se agrava la pena si esta es cometida por medios informáticos. Finalmente se sanciona como contravención la violación al derecho a la intimidad, un derecho que como hemos venido viendo es garantizado y consagrado en la mayoría de la normativa ecuatoriana.

2.1.4 Código Orgánico Integral Penal:

Tomando en consideración que la problemática que gira en torno al marco jurídico si bien ha dado sus inicios en la creación de leyes que contemplen aspectos

significativos a la comisión de actos ilícitos a través de las nuevas tecnologías además de establecerse penas y sanciones en el Código Integral Penal, aun se siente ausencia de legislación, que sea precisa y coherente para el tratamiento de esta nueva modalidad de delincuencia, es decir se busca figuras integrales que en su totalidad resuelvan este tipo de conflictos a través de los diferentes normas tipificadas a lo largo de este código.

El Código Orgánico Integral Penal que entró en vigencia el 10 de agosto del 2014 publicado en el Registro Oficial No 180, toma en consideración nuevas conductas ilícitas, entre estas las cometidas a través de sistemas informáticos. A continuación, se detallará los tipos penales relacionados a delitos informáticos y computacionales que se encuentran legislados por el Código Orgánico Integral Penal:

Delito informático como medio:

1. **Art. 96**.- Tráfico de órganos. - La persona que, fuera de los casos permitidos por la ley, realice actos que tengan por objeto la intermediación onerosa **o negocie por cualquier medio** o traslade órganos, tejidos, fluidos, células, componentes anatómicos o sustancias corporales, será sancionada con pena privativa de libertad de trece a dieciséis años.[10]

Resulta curiosa la aclaración realizada en el Código Orgánico Integral Penal en el artículo antes señalado donde indica que se pueda dar la negociación por cualquier medio. Entiéndase esto que en la actualidad el tráfico de órganos es muy común que sea realizado a través de internet (Bejarano, 2015) (Salazar., 2014), esto debido a que es cometido por bandas dedicadas a la comisión de estos ilícitos desde el continente europeo en Holanda y España. (Salazar., 2014)

2. **Art. 103**.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, **electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos** reales o simulados

[10] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.[11]

3. **Art. 104.-** Comercialización de pornografía con utilización de niñas, niños o adolescentes. - La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, **exporte o venda, por cualquier medio**, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.

Claramente la ley ha dado un gran paso al mencionar que el formato de la pornografía puede ser también en digital, lo que nos permite relacionarlo con un delito informático. Sin embargo, respecto a los medios requerido para la realización de este ilícito la ley las menciona, pero guarda silencio, sabiendo que el internet es una vía que permite la difusión de imágenes a una indeterminada cantidad de personas. Se entiende que la formulación de estos tipos penales mencionados pretenden esencialmente contrarrestar la publicidad y comercialización digital de este material pornográfico. (Lacman, 2016). Las transmisiones de estos delitos se cometen a diario, entre casos conocidos en el país tenemos a GIGATRIBE, una red de pedófilos que a través de una aplicación en el internet tenía a su disposición más de 150GB de pornografía infantil. (Resigner, 2008)

4. **Art. 173**.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos**.- La persona que a través de un medio electrónico** o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años(..)[12]

El articulo 173 menciona claramente que la persona que contacte con finalidad sexual a través de medios electrónicos será sancionado, es importante recalcar la

[11] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

[12] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

puntualización de los legisladores para frenar este tipo de ilícitos que afectan a menores de 18 años.

5. **Art. 178.-** Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en **soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio**, será sancionada con pena privativa de libertad de uno a tres años. [13]

Respecto al artículo señalado anteriormente cabe señalar un tipo caso, como es el Keylogger, que es un programa instalado discretamente en las computadoras de las víctimas en donde se capta todas las pulsaciones electrónicas como cuentas personales de las diferentes redes sociales o peor aún cuentas bancarias, este es la muestra de cómo se viola el derecho a la intimidad a través de los diferentes soportes informáticos y de alguna manera sancionar este tipo de conductas ilícitas cometidas en el país. (López, 2012).

6. **Art. 182**.- Calumnia.- La persona que, **por cualquier medio**, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.

El articulo 182 aclara que quien realiza una falsa imputación por cualquier medio, entiéndase a esta como la utilización de medios informáticos para la consecución de esta clase de delitos será sancionado por nuestra legislación. Algunas veces se entiende que la información que se filtra a través de los diferentes ciberdelincuentes es delicada y es publicada por estos para causar daño a la víctima y se piensa que al utilizar sistemas informáticos de cierta manera se quedara el delito en la impunidad.

7. **Art. 186.-** Estafa. - La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que

[13] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.[14]

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

8. **Art. 188.-** Aprovechamiento ilícito de servicios públicos.- La persona que altere los sistemas de control o aparatos contadores para aprovecharse de los servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo **o de telecomunicaciones,** en beneficio propio o de terceros, o efectúen conexiones directas, destruyan, perforen o manipulen las instalaciones de transporte, comunicación o acceso a los mencionados servicios, será sancionada con pena privativa de libertad de seis meses a dos años.[15]

9. **Art. 190**.- Apropiación fraudulenta por medios electrónicos.- **La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación** de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos,

[14] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[15] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.[16]

En los tres artículos mencionados se entiende que el legislador esta consciente que algunos de los delitos de este tipo son cometidos a través de medios informáticos y por ello en sus diferentes artículos señala de alguna manera la utilización de estos medios, cabe recalcar que algunas veces resulta inútil la existencia de estos tipos penales, puesto que al ser realizados por estos medios es difícil encontrar al autor material del delito, ya que este se encuentra camuflado detrás de un ordenador.

10. **Art. 229.-** Revelación ilegal de base de datos. - **La persona que, en provecho propio o de un tercero, revele información registrada**, contenida en ficheros, archivos, bases de datos o medios semejantes, **a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones;** materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

    Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.[17]

Este tipo penal, busca terminar a todas aquellas conductas orientadas a vulnerar diferentes derechos reconocidos en la Constitución, sin embargo cabe mencionar que uno de los temas principales que recoge el primer inciso del artículo, es que esta conducta será sancionada, si el sujeto que comete el ilícito, es decir el sujeto activo se vale de sistemas informáticos, si no también, telemáticos, o electrónicos, en razón de que para la comisión de un delito de esta índole hace falta el auxilio de Internet, pues muy bien cualquier información de tales características, contenida en cualquier dispositivo de almacenamiento., puede ser difundida por cualquier medio de comunicación, que en este caso pueden ser medios informáticos.

[16] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

[17] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

11. **Artículo 211.-** Supresión, alteración o suposición de la identidad y estado civil.- **La persona que ilegalmente impida, altere, suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos,** partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años. [18]
12. **Artículo 212.-** Suplantación de identidad. - **La persona que de cualquier forma suplante la identidad** de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. [19]

En el presente artículo de la carta magna de la República del Ecuador, pretende precautelar la manipulación de datos correspondientes al Registro Civil, nos permite entender la utilización de los sistemas informáticos como medio para la consecución de un fin negativo que en este caso sería, la alteración de datos correspondientes al registro a través de sistemas informáticos. Seguido del articulo doscientos doce donde lo importante es la integridad de la persona puesto que esta podría verse afectada por cualquier medio si es que se llegara a dar el caso de una suplantación de identidad, en ambos casos se sancionaran las conductas antes mencionadas con uno a tres años de prisión, lo que de alguna manera espera detenga o disminuya la comisión de este ilícito.

13. **Artículo 213.-** Tráfico ilícito de migrantes.- **La persona que, con el fin de obtener directa o indirectamente beneficio económico u otro de orden material por cualquier medio,** promueva, capte, acoja, facilite, induzca, financie, colabore, participe o ayude a la migración ilícita de personas nacionales o extranjeras, desde el territorio del Estado ecuatoriano hacia otros países o viceversa o, facilite su permanencia

[18] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[19] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

irregular en el país, siempre que ello no constituya infracción más grave, será sancionada con pena privativa de libertad de siete a diez años.[20]

Al igual que en los artículos mencionados a lo largo de este capítulo, los sistemas informáticos son utilizados como medio para la comisión del acto ilícito, tomando en cuenta que en este tipo penal, a través de las redes de información se forman grandes mafias que se encargan de la consecución de este tipo de conductas. Se entiende que este tipo penal es de preocupación global, pues afecta a gran número de países en el mundo, estos son vulnerables a la explotación y mediante la red de internet se ha facilitado la realización de este, ya que este un crimen organizado trasnacional. (Artola, 2007)

14. **Artículo 231**.- Transferencia electrónica de activo patrimonial. - **La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos,** para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. [21]

Este tipo penal busca limitar la conducta ilícita referente al funcionamiento de sistemas informáticos que se encargan de regular la transferencia de archivos de activos patrimoniales, al igual que en los anteriores este utiliza como medio a los sistemas informáticos para la consecución de esta, es importante mencionar que la brecha que se ha generado por el acceso tan facilitado al sistema de información nos deja un reto grande acerca de la cultura informática, que debería ser aplicada por cada uno de los usuarios de este servicio.

[20] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[21] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

15. **Artículo 233.-** Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. **La o el servidor público que, utilizando cualquier medio electrónico o informático,** obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. (..)[22]

Este tipo penal tiene un sujeto activo en particular que viene a ser, cualquier servidor público, en esta, su conducta debera un daño a información clasificada y use a los sistemas informáticos como medio para la consecución de este ilícito. Lo que resulta interesante es que el medio informático, que sea utilizado para la comisión de este ilícito no sea solo para la difusión sino para la obtención de los mismos, es decir que a dentro del mismo tipo penal se busca precautelar la información clasifica desde su obtención hasta su difusión.

16. **Artículo 299**.- Defraudación aduanera.- La persona que perjudique a la administración aduanera en las recaudaciones de tributos, sobre mercancías cuya cuantía sea superior a ciento cincuenta salarios básicos unificados del trabajador en general, será sancionada con pena privativa de libertad de tres a cinco años y multa de hasta diez veces el valor de los tributos que se pretendió evadir, si realiza cualesquiera de los siguientes actos:[23]

    6. **Induzca, por cualquier medio, al error a la administración aduanera(..)**

17. **Art. 365**.- Apología.- **La persona que por cualquier medio haga apología de un delito** o de una persona sentenciada por un delito, será sancionada con pena privativa de libertad de quince a treinta días.[24]

[22] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[23] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[24] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

Dentro de este tipo penal, aunque resulte muy amplio, cabe la posibilidad de la comisión de un delito informático, ya que, mediante los sistemas de información actual, siendo este el internet, que con un gran número de visitas diarias se han presentado ataques raciales o sexistas, o algunos casos dentro del contexto de la palabra odio que a través de la historia se han presentado manifestaciones peyorativas en contra de ciertos grupos sociales de la sociedad.

18. **Artículo 396.-** Contravenciones de cuarta clase.- Será sancionada con pena privativa de libertad de quince a treinta días:[25]
    1. **La persona que, por cualquier medio, profiera expresiones en descrédito o deshonra en contra de otra.**

Para terminar la enumeración de los delitos informáticos como medio, es importante mencionar al tipo penal que recae sobre las contravenciones, en las cuales se busca prevenir la utilización de medios informáticos para proferir expresiones de descrito en contra de otra persona. Es decir, la utilización de medios informáticos para producir deshonra a otro ser humano.

Delito informático como fin:

El Código Integral Penal brinda ciertas normas que pueden ser utilizadas para contrarrestar estas conductas, sin embargo, la finalidad de esta sección es mencionar los delitos informáticos tipificados y tiene como fin el daño a un sistema informático y buscar la manera de hacer más efectiva la materia legislativa existente para solucionar este tipo de delitos.

Frente a lo expuesto en el párrafo anterior, existe una gran posibilidad, que por medio del uso indebido de la informática de paso a la manipulación de diferentes sistemas, como pueden ser: hospitales, bancos, aeropuertos y muchos más en donde el grado de afectación en la sociedad puede ser mayor (Bequai, 1996., pág. 48). La brecha a la consecución de estos delitos es enorme, por este motivo es necesario dentro de nuestro país que la fiscalía en cumplimiento de su mandato dote de las herramientas que generen eficacia en la normativa penal.

[25] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

Esta parte de tipos penales hace un enfoque directo en el delito informático, puesto que se entiende, que esta categoría se enmarcan todas aquellas conductas criminales que van dirigidas a las computadoras, accesorios o programas. Esto hace referencia a todos aquellos sujetos que utilizan la tecnología electrónica como fin u actividad delictiva para causar daño a la misma.

1. **Artículo 191**.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. [26]
2. **Artículo 192.-** Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan Código Orgánico Integral Penal 85 información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. [27]
3. **Artículo 193.-** Reemplazo de identificación de terminales móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años. [28]
4. **Artículo 194**.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. [29]
5. **Artículo 195**.- Infraestructura ilícita.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que

[26] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[27] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[28] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[29] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años.[30]

6. **Art. 230.-** Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

   La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
   La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
   La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.[31]

7. **Artículo 232.-** Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.[32]

---

[30] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[31] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[32] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

8. **Artículo 234.-** Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.[33]
9. **Artículo 298**.- Defraudación tributaria.- La persona que simule, oculte, omita, falsee o engañe en la determinación de la obligación tributaria, para dejar de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero, será sancionada cuando:

   8. Altere libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.
   9. Lleve doble contabilidad con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica.
   10. Destruya total o parcialmente, los libros o registros informáticos de contabilidad u otros exigidos por las normas tributarias o los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias.[34]

2.1.5 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación:

"El principio fundamental es que el conocimiento es universal, es patrimonio de la humanidad. No puede ni debe ser privatizado" (Correa, 2016). En el mes de diciembre del presente año, se publicó en el Registro Oficial un nuevo Código relativo al pasado referente a propiedad intelectual, La aparición de este da apertura a la sociedad de

[33] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.
[34] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

información al internet, como lo menciona el presidente de la Republica, el conocimiento es un patrimonio y el acceso al internet para permitir el desarrollo del mismo debe encontrarse al alcance de todos.

Este Código busca llevar a nivel de normas lo que se planteó como objetivo en el Plan Nacional del Buen Vivir,[35]a través de este se busca la construcción de un sistema social que nos brinde un acceso igualitario a las herramientas informáticas para desarrollar inclusión al conocimiento. Es por ello que dentro del capítulo dos, que busca el acceso y soberanía del conocimiento en entornos digitales e informáticos en su artículo 39[36], redacta sobre el acceso universal a los entornos digitales, por el mismo hecho de brindar el acceso a los sistemas de información, el mismo estado debe brindar los mecanismos de control para la efectividad para la efectividad de las normas. El artículo 40 del mismo nos menciona el acceso al internet como un servicio básico que debe ser de calidad y accesible para todos.[37]

A lo largo del mismo Código existen artículos que explican el funcionamiento del acceso al Internet, al igual que Derechos de autor de carácter informático, protecciones al mismo y lo que llegase a pasar si estos fuesen violados. Al ser un código actual trata de adecuarse a la realidad de sociedad de información ecuatoriana para precautelar todos los derechos que se pudiesen violar con la intromisión tecnológica a la red de internet. Tal es el caso que en el Apartado III del presente código hace referencia al uso indebido de derechos de Propiedad Intelectual en la Internet, estos artículos se ven abarcados del 584 al 586, en estos se habla del ejercicio de la acción, factores para

[35] Dentro de lo enmarcado en el Plan Nacional de vivir se plantea el acceso al Internet a todos, esto se encuentra planteado en el primer objetivo que se basa en consolidar el Estado democrático y la construcción del poder popular, en su inciso 5.5.K en el cual se busca garantizar el acceso a esta herramienta tecnológica a todos.

[36] **Artículo 39.-** Acceso universal, libre y seguro al conocimiento en entornos digitales.- El acceso al conocimiento libre y seguro en entornos digitales e informáticos, mediante las tecnologías de la información y comunicaciones desarrolladas en plataformas compatibles entre sí; así como el despliegue en infraestructura de telecomunicaciones, el desarrollo de contenidos y aplicaciones digitales y la apropiación de tecnologías, constituyen un elemento transversal de la economía social de los conocimientos, la creatividad y la innovación y es indispensable para lograr la satisfacción de necesidades y el efectivo goce de derechos. El acceso universal, libre y seguro al conocimiento en entornos digitales es un derecho de las y los ciudadanos

[37] Artículo 40.- Acceso a Internet. - El Estado garantizará el acceso universal al servicio público de internet en los términos previstos en la Constitución de la República. Los organismos competentes vigilarán que el precio de este servicio sea equitativo, y establecerán los mecanismos de control y regulación correspondientes.

considerar la intención de la mala fe, los factores para considerar un legítimo nombre de dominio y la sanción para la misma.[38]

Una de las partes del código que llama mi atención se centra en el libro III que estipula la gestión del conocimiento, en esta sección el artículo 136 del presente código en el que se estipula lo siguiente: "Artículo 136.- Uso lícito del software. - Salvo pacto en contrario, será lícito el aprovechamiento del software para su uso en varias estaciones de trabajo mediante la instalación de redes, estaciones de trabajo u otros procedimientos similares."[39] En concordancia a lo estipulado en el presente capitulo se le permite a la sociedad el acceso libre al software, esto también está estipulado en un decreto legislativo que nos permite y brinda la oportunidad de acceso igualitario a este sistema informático, el mismo hecho de permitir este libre acceso debe generar la suficiente conciencia en la sociedad en respetar este ámbito o que se brinden los mecanismos necesarios para garantizar este derecho y evitar las conductas que adolezcan este derecho.

En suma, la reciente publicación del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, planta elementos de avanzada respecto a la garantía del derecho al acceso de internet. Sin embargo, debe tenerse en cuenta que la implementación de programas de software libre o abierto no aseguran que las personas o las empresas, necesiten o encuentren alicientes en dejar de utilizar software privado para aplicar programas informáticos de código abierto, ya que existe una percepción de que, si bien el software libre es de conocimiento público, los de carácter privado suelen funcionar mejor. Es decir, el hecho de generar esta apertura que en su momento se lo hizo a través de decreto, queda en consideración de las partes su utilización, por lo que pierde eficacia.

2.1.6 Decretos:

[38] Artículo 584.- De la Acción.- El propietario de una marca u otro derecho de propiedad intelectual podrá iniciar una acción de tutela administrativa, si, un tercero, sin el consentimiento del titular, intenta de mala fe sacar provecho del derecho de propiedad intelectual y registra, comercializa, o utiliza un nombre de dominio que al tiempo del registro del nombre de dominio: a) haya sido idéntico o similar con una marca u otro derecho de propiedad intelectual reconocido en el país; o, b) sea capaz de causar dilución con una marca notoriamente conocida en el país. Obtenido en Registro Oficial 09-12-2016 Año IV No 899. Acceso: 20-12-2016.

[39] Articulo 136 Obtenido en Registro Oficial 09-12-2016 Año IV No 899. Acceso: 20-12-2016.

Un punto clave dentro del marco legal ecuatoriano es el Decreto Ejecutivo No. 1014 emitido el 10 de abril de 2008[40], donde se dispone el uso de Software Libre en los sistemas y equipamientos informáticos de la Administración Pública de Ecuador. Es interés del Gobierno ecuatoriano alcanzar soberanía y autonomía tecnológica, esto puede ir de la mano con el articulo 16 antes mencionado donde se garantiza el acceso universal a las tecnologías al igual que el estado busca de cierta manera este acceso mediante este decreto.

Lo que se pretende con este decreto es la utilización de estándares abiertos del software informático, la minimización de compra de licencias propietarias, la contratación de servicios en proyectos informáticos, la reutilización del software y el uso preferencial de programas navegadores como medios de acceso para que la sociedad de información ecuatoriana siempre este en un desarrollo adecuado y positivo.

Si bien es cierto esta figurada que fue adoptada con anterioridad en el 2008, en la actualidad vuelve a ser tomada en cuenta como ya fue explicado en la sección del Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, es una tendencia bastante llamativa, puesto que genera dudas acerca de decisión frente al tipo de software que se desea poseer, sin embargo como lo mencione con anterioridad esta figura se vuelve ineficiente por motivos de seguridad de las empresas con la evidente diferente de que esta figura del decreto solo se aplica a entidades del sector público, respecto a todo esto debe entenderse que muchas de las ventajas y desventajas de la utilización de software libre son debidas a su reciente nacimiento, lo que se considera que muchas de ellas desaparecerán en mediano plazo, porque al ser una tendencia de los últimos diez años aun precisa de mucho más estudio para su correcta utilización.

2.2 Practica Judicial/Proceso Penal:

2.2.1 Jurisdicción en territorio Digital:

[40] Decreto Ejecutivo No. 1014 emitido el 10 de abril de 2008 – El uso de Software Libre en los sistemas y equipamiento informáticos de Administración Publica de Ecuador. Acceso en: 19-12-2016.

En lo que respecta a materia penal informática, se entiende que los delitos informáticos al ser cometidos a través de sistemas informáticos se deben tener en cuenta que resulta bastante complicado llegar a determinar el lugar exacto de la comisión del ilícito y la persona o procedencia en donde se suscitó, tal acción. Se entiende que la jurisdicción, es la potestad publica de juzgar y hacer ejecutar lo juzgado, por lo que dentro del proceso respectivo el juez debe tomar las medidas suficientes para no dejar en la impunidad estos ilícitos, aun sabiendo que en un alto porcentaje conocer al autor del mismo resulta un verdadero desafío.

A partir de esto, basándonos en el estudiado principio de territorialidad, donde se señala que la jurisdicción en materia penal radica en el lugar donde se ha cometido la infracción y en algunos casos donde se encuentra el bien jurídico afectado (Sacchetto, 2005, pág. 35), garantizando la competencia estipulada por el Código Orgánico Integral Penal en el artículo 404[41], sin embargo en lo que respecta a los delitos informáticos, no se puede diferenciar estos puntos mencionados anteriormente, por lo que a la lógica se entendería que al no conocer el lugar exacto de la comisión del ilícito, la jurisdicción aplicable para estos casos respondería al lugar donde se encuentra ubicado el bien jurídico afectado en este ilícito, esto en el caso, que de manera extraordinaria se conociera el lugar exacto de la comisión del ilícito.

Durante todo el proceso investigativo de esta disertación se ha determinado que los delitos informáticos son figuras fuera del campo tradicional en materia penal donde se presentan varios retos por el hecho de ser cometidos fuera de no nuestro alcance visual, sin tomar en cuenta que, una parte fundamental de un proceso es tener claro cuáles son las pautas para empezar a juzgar el ilícito, por ello considero que es fundamental que el juez sea una persona que conozca y sea participe activa de la cultura

[41] "Artículo 404.- Reglas de la competencia. - Para determinar la competencia de la o el juzgador, se observarán las siguientes reglas:
1. Hay competencia de la o el juzgador cuando se ha cometido la infracción en la circunscripción territorial en la que este ejerce sus funciones. Si hay varios juzgadores, la competencia se asignará de conformidad con el procedimiento establecido por la ley.
2. Cuando la infracción se ha preparado e iniciado en un lugar y consumado en otro, el conocimiento de la causa corresponde a la o al juzgador de este último.
3. Cuando no es posible determinar el lugar de la comisión de la infracción o esta se ha cometido en circunscripciones territoriales distintas o inciertas, será competente la o el juzgador:
a) Del lugar en que la persona es aprehendida o detenida.
b) Del lugar del domicilio de la persona procesada, aunque se encuentre prófuga.
c) De la capital de la República, si no es posible determinar domicilio." Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. *República del Ecuador*.

de información para que sea realista al momento de tomar decisiones con lo que respecta a estos ilícitos.

2.2.2 Sujetos Procesales:

SUJETOS PRINCIPALES:

Sujeto Activo – Sospechoso:

El sujeto activo o sospechoso es la persona a que se le acusa por cometer un delito que implica la desobediencia de la norma, es decir la contradicción de lo interpuesto por parte del ordenamiento jurídico para la coexistencia de la sociedad. En cuanto respecta los delitos informáticos, de manera general, la sociedad lo conoce al sujeto activo como el "hacker", quien es el sujeto con ciertas habilidades especiales para el manejo de sistemas informático y que en algunos casos por su situación económica o laboral debe realizar ciertas actividades estratégicas de carácter sensible o en otros casos solo son personas hábiles con los sistemas de información y dentro de sus actividades se encuentra la comisión de actos ilícitos en la red por cuestiones personales. (Lacman, 2016)

La víctima:

El sujeto pasivo es la persona que fue violentado en uno o algunos de sus derechos. Esta persona pudo haber sido agraviada a través de un medio físico, o en este caso digital. Es decir, la víctima es la persona sobre la que se da la acción antijurídica cometida por el sujeto activo. En los delitos informáticos se entiende que la víctima es la persona que fue perjudicada a través de la computadora o cualquier sistema informático y ha sido vulnerado ciertos derechos que le son pertenecientes.

La Fiscalía:

Dentro de la fiscalía el gestor de justicia, es el fiscal, este sujeto procesal es quien dirige la investigación del delito y es la persona interviniente a nombre del Estado, hasta la finalización del proceso. Durante el periodo de la investigación el fiscal cumple una figura sumamente importante, ya que este es el medio de todas las

diligencias que se realizan en el trayecto de la investigación del delito informático. Es importante mencionar que, en el ámbito de los delitos informáticos, el conocimiento y experiencia del fiscal dentro de esta materia es uno de los factores más importantes, ya que, de esta manera, se encontrara una vía satisfactoria para encontrar todos los elementos para que el juez logre dar un dictamen favorable. (Acurio, 2015). En el Ecuador existen pocos fiscales que pueden manejar este tipo de casos, debido a que no poseen las herramientas, ni los conocimientos necesarios para la solución de este tipo de actuaciones, por lo que los resultados en este tipo de casos, es desfavorable e ineficiente para las víctimas.

Abogado de la Defensa:

En el marco de los delitos informáticos, el papel del abogado es un factor importante, ya que no todos los abogados tienen conocimientos del derecho penal informático y a través de las actuaciones de este se puede solicitar todo lo necesario para que el dictamen sea favorable para su cliente. Al igual que los fiscales, en el país existen pocos abogados que tienen capacitación actualizada referente a estos temas, en el caso de poseer un abogado que tenga conocimientos acerca de los delitos informáticos, se crea una gran ventaja ya que este conoce el resultado y todo lo que puede solicitar para un dictamen positivo, sabiendo que un abogado no especializado podrá tener muchas fallas y puede causar daños a su cliente.

SUJETOS AUXILIARES:

Los Peritos Informáticos:

El perito informático es el profesional, que en su función debe asesorar al juez respecto a los temas informáticos. De acuerdo a lo que dispone el artículo 511 del Código Integral Penal "son profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura." [42]Este sujeto debe analizar todos los elementos

[42] Art. 511.- Reglas generales.- Las y los peritos deberán:
1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.
2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.
3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.

importantes de la intervención al sistema telemático para encontrar todos los datos que puedan establecer una prueba o indicio efectivo para el litigio. (Salamanca, 2013).

Lo interesante del perito informático, es que este debe regirse por algunos principios para encontrar sus indicios, siento estos:

1. Objetividad: "Debe investigar también las circunstancias que sirvan de descargo.(..) "La Fiscalía tiene que averiguar los hechos; para ello, tiene que reunir con el mismo empeño, tanto los elementos de cargo como los de descargo." (Claus, 2006, págs. 53-330)
2. Autenticidad y Conservación: "Durante la investigación, se debe conservar la autenticidad e integridad de los medios probatorios." (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017)
3. Legalidad: "El perito debe ser preciso en sus observaciones, opiniones y resultados, conocer la legislación respecto de sus actividades periciales y cumplir con los requisitos establecidos por ella". (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017)
4. Idoneidad: "Los medios probatorios deben ser auténticos, ser relevantes y suficientes para el caso". (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017)
5. Inalterabilidad: "En todos los casos, existirá una cadena de custodia debidamente asegurada que demuestre que los medios no han sido modificados

---

4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito qu e lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.
5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.
6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje, identifica ción del perito,
descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilu straciones gráficas cuando corresponda, las conclusiones y la firma. 7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes,
para lo cual podrán emplear cualquier medio.
8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por es tas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.
De no existir persona acreditada como perito en determinadas áreas, se deberá contar con quien tenga con ocimiento,
especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje. Para los casos de ml a práctica
profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organ smo rector de la materia.
Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados co mo prueba, através de testimonios anticipados o podrán ser receptados mediante video conferencias de ac uerdo a las reglas del presente Código.

durante la pericia." (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017)

6. Documentación: "Deberá establecerse por escrito los pasos dados en el procedimiento pericial" (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017)

Estos principios deben ser cumplidos a cabalidad ya que la existencia de este sujeto dentro del proceso de investigación es de alta importancia. En cuanto respecta a la objetividad el perito debe regirse a los códigos de ética profesional, para que durante el principio de autenticidad exista la integridad de los medios probatorios. El principio de legalidad es otro punto necesario debido a que el perito debe ser concreto en sus observaciones, opiniones y resultados además de tener un claro conocimiento de la legislación en lo que concierne a materia del delito informático. Todo medio probatorio debe ser auténtico y en todo el procedimiento existirá una cadena de custodia debidamente asegurada que va permitir al fiscal demostrar que todos los medios probatorios no fueron alterados durante la pericia y durante todo el procedimiento pericial. (Acurio, 2015, pág. 233)

Testigos:

Es un sujeto procesal que nos permite conocer de cierta forma alguna parte relativa al delito, la información proporcionada por el testigo nos permite verificar ciertos indicios referentes a los delitos informáticos. Toda la información vertida por parte de los testigos son un medio probatorio efectivo para encontrar un dictamen que sea objetivo y puntual. (Cuenca, 2014, pág. 64) Es decir, todo lo expuesto por los testigos son elementos impactantes en el procedimiento, en algunos casos el testigo no solo tiene el poder de informar sino de influir en las emociones del juez (Possley, 2016), ya que al final, este es el que dicta sentencia.

2.2.3 Investigación Penal

Respecto a la investigación penal como menciona Acurio, es imperioso recordar lo que proclama el primer artículo de la Constitución de la Republica[43] donde se

[43] Art.1.- El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada.

establece que el Ecuador es un Estado Constitucional de derechos y justicia, al hablar de justicia es un punto sumamente ponderador (Acurio, 2015, pág. 167), ya que por conocimiento en materia penal se sabe que en nuestro país nos encontramos con un sistema de mínima intervención penal, ya que no se persigue al ciudadano como un objeto de persecución sino que se busca devolverle su dignidad.

La oficina de las Naciones Unidas contra la Droga y el Delito, nos menciona respecto a la investigación penal:

"la investigación de delitos es el proceso por el cual se descubre el autor de un delito, cometido o planeado, mediante la reunión de hechos (pruebas) , si bien también puede suponer la determinación, ante todo, de si ha cometido o no un delito. La investigación puede ser reactiva, es decir, aplicada a delitos que ya han perpetrado, o proactiva, encaminada a cierta actividad planificada para el futuro." (UNDOC, 2010)

Los delincuentes informáticos usan la tecnología como fin o medio para facilitar el cometimiento de las infracciones y así poder evitar a las autoridades y dejar en la impunidad este tipo de actuaciones. Esto ha hecho que la Fiscalía y la Función Judicial busquen la manera de capacitarse en temas relacionados a la sociedad de información con acceso a la tecnología, ya que las computadoras y los otros medios telemáticos pueden ser utilizados también por parte de los gestores de justicia para la contrarrestar la ejecución del delito y hallar a la persona que lo realizó. (Acurio, 2015, pág. 170)

La falta de herramientas necesarias para combatir estas conductas, es un tema que preocupa no solo al Ecuador, ya que esto implica la falta de elementos de seguridad y ha generado varios casos polémicos alrededor del mundo debido a la intromisión tecnológica a la red de internet. Si bien es cierto el Código Integral Penal integra mecanismos que buscan contrarrestar este tipo de conductas para disminuir o erradicar la existencia de estas. En nuestro marco jurídico la investigación penal es encabezada por el fiscal, sujeto que mencionaremos a posterioridad, este en conjunto a la policía judicial y al grupo de investigadores civiles de la Dirección Nacional de Investigaciones de la Fiscalía General del Estado.

Este proceso investigativo penal está comprendido por los siguientes puntos:

1. Investigación Penal.
2. Investigación Criminalística.

3. Investigación Criminológica.
4. Administración de la Información de Investigación Penal. (Acurio, 2015, pág. 171).

Lo característico de esta investigación es su continuidad y con puntos especiales que requiere una larga planeación que contenga todos los pasos necesarios para no dejar esta clase de actos ilícitos en la impunidad, siendo necesario e conocimiento del hecho, los actos urgentes seguido por la planeación de la investigación, la consolidación de los elementos de convicción finalizando con los informes respecto a la investigación.

Una parte fundamental de este proceso de investigación recae en un principio universal del sistema penal, donde se indica que los sospechosos son inocentes hasta que se prueba su culpabilidad, donde en base a todos los puntos estipulados con anterioridad debe existir una evaluación objetiva de los hechos y que no haya existido manipulación de estos para ajustarlos a las sospechas de quienes se encuentran investigándolos. (Aez, 2010). Dentro de este proceso es imperioso la existencia de pruebas, ya que con esta se confirma o se niega en su totalidad la hipótesis o lo que se encontraba sabiendo que el principio de información es un valor económico con relevancia jurídico- penal. (Acurio, 2015, pág. 172)

Para que este tipo de acciones pase a conocimientos de los gestores de justicia existen dos vías impuestas por el estado siendo estas: la denuncia y la acusación particular. La denuncia se da en razón de la persona que conociendo el cometimiento del delito puede presentar su denuncia en la fiscalía, en el sistema integral de investigación o ante el órgano correspondiente para la presente investigación. Mientras que la acusación particular, la realiza la victima de la acción como persona natural o a través de su abogado, en caso de ser una persona jurídica esta deberá hacerlo a través de su representante legal para dar a conocer y seguir el procedimiento correspondiente. (Cuenca, 2014, pág. 60)

Cabe mencionar que en este tipo de investigaciones para lo que es considerado un delito informático existe una anomia que no solo se basa en la infracción por parte del sujeto activo, sino que este cree que al encontrarse en el ciberespacio no posee una vinculación con el derecho, sabiendo que esta vinculación es estrecha pero deficiente donde las etapas o procedimientos establecidos por los gestores de justicia no resultan

efectivos a momento de tratar una actuación ilícita que comprenda la utilización de sistemas informáticos. (Ballesteros, 2014, pág. 232)

2.2.4 Investigación en la escena:

El lugar de la comisión del acto ilícito es el marco de inicio de una investigación pericial, en este debe existir una investigación exhaustiva donde se aplica el principio criminalística de transferencia[44]. En algunos casos los peritos no son los primeros en llegar a la escena del delito, cuando estos deberían darle la importancia necesaria y ser los primeros en llegar por la importancia que representan. Dentro del procedimiento que se debe cubrir ciertos parámetros y requisitos que son: (Acurio, 2015, págs. 249-250)

1. Observar y establecer los parámetros de la escena del delito.
2. Tomar medidas de seguridad.
3. Facilitar primeros auxilios, de ser necesarios en el caso.
4. Aseguramiento físico de la escena.
5. Aseguramiento de todas las evidencias.
6. Entregar la escena del delito
7. Documentos de la explotación de la escena.

Al momento de dar cumplimiento todas estas responsabilidades, se llega a dar una reconstrucción efectiva de la escena del crimen. Cada factor es importante para encontrar los elementos necesarios para generar un indicio adecuado. Sin embargo, existe una particularidad con el aseguramiento físico de las evidencias, donde debe existir una cadena de custodia, esta se entiende como un sistema que permite asegurar a las mismas, basado en el principio de mismidad, que busca garantizar la autenticidad de las pruebas para que el sistema realizado no se vuelva ineficaz durante el proceso. Dentro de la investigación de la escena del crimen es indispensable que sea documentada cada etapa de este proceso para poder tener un registro de lo todo lo suscitado y que esto sea favorable como ya se ha mencionado para encontrar elementos de convicción efectivos que conlleven a un dictamen favorable por parte del juez.

[44] El Principio de Transferencia, también denominado de intercambio, y que consiste en la transición de los indicios encontrados en la escena del crimen y el cuerpo de la víctima, una vez analizada por los peritos forenses, y aceptada por las autoridades judiciales pasa a ser prueba, su aplicación conduce a descubrimientos determinantes de lo sucedido entorno a la escena del crimen y del cuerpo de la víctima. Acceso en: Criminologia - http://dspace.utpl.edu.ec/bitstream/123456789/12994/1/Barrera_Alvarado_Johanna_del_Rocio.pdf (02-01-2017)

2.2.5 Elementos de Convicción:

A un acto se lo determine como punible cuando este sea compuesto por algunos elementos de convicción que también son conocidos como prueba digital. Estos elementos de convicción son el grupo de pruebas que en el caso de lo que corresponde los delitos informáticos son necesarios para probar la existencia y la materialidad del delito, además de ser considerados una de las facetas más útiles dentro de la investigación criminal, sabiendo que sin esta queda sin efecto todo el procedimiento ya que se entiende que es imposible delimitar el delito y considerarlo punible para que no quede en la impunidad. Todos estos elementos de convicción deben ser idóneos y veraces al momento de ser presentadas en audiencia además de tener como anexo un informe por parte del perito que avale a la misma. (Acurio, Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0, 2017, pág. 1)

En materia penal de carácter informático resulta un poco dificultoso precisar y señalar específicamente los elementos de convicción ya que para esto existen hechos diferentes y existe una brecha más grande cuando estos son realizados a través de medios virtuales, debido a que no existen fronteras en los sistemas informáticos y existe gran dificultad para encontrar al operador del delito. Por ello cada prueba analizada por un perito informático es parte esencial para obtener un proceso impoluto, conciso y objetivo sin que, de alguna manera, este afecte el interés de alguna de las partes.

Un punto fundamental en esto, es la valoración de la prueba, esto dice mucho ya que la decisión tomada se basará en la relación del grado de eficacia de la misma, debido a que la prueba siempre va influir directamente en la decisión del juez, esta debe establecer materialmente los hechos y la función intelectual del juez en esta parte juega un rol predominante, conociendo que solo a él le compete efectuar observaciones exclusivas sobre esta prueba. Para poder valorar las pruebas los jueces deben tener en cuenta cierto sistemas, partiendo de la libre convicción donde la prueba se basa en el libre arbitrio del juez, aunque en la actualidad, este sistema ya no es tomado en cuenta. Otro de los sistemas, es el también conocido como, sistema legal, en esta se debe cumplir ciertos parámetros ya que la ley es la que expresa debidamente lo que se debe considerar.

Un sistema de prueba bastante característico, es el de la sana critica, sistema donde se otorga la libertad al juez para apreciar la eficacia de las pruebas producidas, sino a través de un análisis razonado, tomando en cuenta reglas de sentido y el entendimiento exigiéndole la fundamentación de sus respuestas y resoluciones. Entonces se puede concluir que la circunstancia propia del desarrollo de la tecnología precisa la existencia de un sistema mixto, que combine la sana crítica y el sistema tasado, lo que llevaría a una prueba pericial más completa.

Capítulo 3: Caso práctico.

3.1. Justificación

Clarificar el momento y hora exacta en la que se comete un delito informático resulta un tema de ardua investigación, debido a la falta de mecanismos necesarios para sancionar al mismo. (Acurio, 2010) La libertad de información de Internet es el argumento en cuestión, porque se debe garantizar la integridad de la misma para que no existan daños en contra de los usuarios de la red como robo o suplantación de identidad y utilización de la misma para fines ilícitos (Voluntad Digital, 2017). En vista de esto, surge la necesidad de estudiar dos casos suscitados en Ecuador que escenifican la realidad respecto a casos que se encuentran bajo el mismo tipo penal, correspondiendo este a los delitos informáticos, donde consecuentemente puede llegar a existir un doble estándar en referencia a las resoluciones judiciales sobre la incorrecta o incongruente aplicación de la ley en casos similares.

La aparición de los delitos informáticos, genera diferentes temas a ser debatidos dentro de lo que se contempla en el marco legal, esto debido a que al observar al "hacker" como un sujeto activo delito se debe reconocer a este, haciendo alusión a que su conducta debe adecuarse al tipo penal para ser punible, recalcando que, en ambos casos a ser analizados los sujetos activos, son periodistas, por lo que es necesario contemplar a la luz de la Ley Orgánica de Comunicación lo que se entiende por libertad de expresión, esta normativa señala en su artículo 17 "El Derecho a la libertad de expresión y opinión.- Todas las personas tienen derecho a expresarse y opinar libremente de cualquier forma y por cualquier medio, y serán responsables por sus expresiones de acuerdo a la ley."[45]

Dado los parámetros contemplados por la Ley Orgánica de Comunicación se entiende que su rol dentro de la sociedad se basa en la difusión de información o noticias de interés para la sociedad, de la manera más objetiva posible, para que no existan razones que provocan incertidumbre en la veracidad de lo difundido. Existen

[45] Oficial, Registro. "Órgano del Gobierno del Ecuador." Ley Orgánica de Comunicación. Registro Oficial 22 (2011).

diferentes formas de analizar este tema, desde puntos opuestos donde la actividad del "hacking" puede ser catalogada como positiva o negativa, pero siempre dependerá del grupo focalizado de la sociedad al que se pertenece. (Raul Martin, 2015).

La sociedad ecuatoriana es participe de la cultura tecnológica a través del acceso al internet garantizado en nuestro ordenamiento jurídico como se mencionó en el capítulo anterior[46], dentro de la misma legislación ecuatoriana existen anomias[47] que provocan conflictos al momento de sancionar estas conductas. Nuestro Código Orgánico Integral Penal señala en su artículo 10: "Son infracciones los actos imputables sancionados por las leyes penales, y se dividen en delitos y contravenciones, según la naturaleza de la pena peculiar" (Registro Oficial, 2013). En aplicación al principio de legalidad[48], nuestro ordenamiento jurídico determina que un comportamiento es considerado punible siempre y se encuentre tipificado; al poder analizar ambos casos, se verifica la existencia elementos de convicción necesarios para que las conductas sean sancionados por la ley ecuatoriana. Sin embargo, el enfoque que se le otorga a cada caso es completamente diferente a pesar de encontrarse bajo el mismo tipo penal.

En referencia al caso de "WikiLeaks" en contraposición al de Fernando Villavicencio se buscará los argumentos que generaron la discrepancia dentro del ordenamiento jurídico donde el sujeto activo del caso WikiLeaks, siendo este Julián Assange no tuvo ningún tipo de sanción por su conducta, mientras que al ecuatoriano

---

[46] **Artículo 39.-** Acceso universal, libre y seguro al conocimiento en entornos digitales.- El acceso al conocimiento libre y seguro en entornos digitales e informáticos, mediante las tecnologías de la información y comunicaciones desarrolladas en plataformas compatibles entre sí; así como el despliegue en infraestructura de telecomunicaciones, el desarrollo de contenidos y aplicaciones digitales y la apropiación de tecnologías, constituyen un elemento transversal de la economía social de los conocimientos, la creatividad y la innovación y es indispensable para lograr la satisfacción de necesidades y el efectivo goce de derechos. El acceso universal, libre y seguro al conocimiento en entornos digitales es un derecho de las y los ciudadanos

Artículo 40.- Acceso a Internet. - El Estado garantizará el acceso universal al servicio público de internet en los términos previstos en la Constitución de la República. Los organismos competentes vigilarán que el precio de este servicio sea equitativo, y establecerán los mecanismos de control y regulación correspondientes. (Obtenido del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, Ecuador, 2017)

[47] "Anomia" es uno de los conceptos y temas de la sociología con lo cual trabaja el jurista sociólogo (obviamente hay muchos otros, tales como el "control social", "cambios", "conflicto", "legitimidad", "estrato", "clase", a los cuales haremos referencia en otros capítulos). Anomia es una palabra griega que es usada en casi todos los idiomas de la cultura occidental. A-nomia significa literalmente ausencia de ley. Obtenido de: http://www.arnaldomartinez.net/sociologia/unidad04.pdf (17-01-2107.)

[48] "El Principio de Legalidad se basa en que ningún hecho puede ser considerado punible si no existe ley anterior que haya previsto esto. "[…]sólo las leyes pueden decretar las penas de los delitos; y que esta autoridad no puede residir mas que en el legislador que representa aun toda la sociedad agrupada por una contrato social. […]" (Obtenido de Beccaria, Cesare, De los delitos y de las Penas, Bogotá, Colombia: Temis, 3ra, 2005, pagina 74).

Fernando Villavicencio[49] se han encontrado los diferentes mecanismos para privarlo de libertad y sancionar su conducta. Siendo este el factor de estudio de los casos antes mencionados que permite determinar los límites y excepciones al acceso de la red de internet a la luz del Código Orgánico Integral Penal

Tanto en el caso de Assange y en el de Villavicencio existió la divulgación de correos electrónicos con interés público. Sin embargo, dentro de lo que compete para Julián Assange, este tipo de información se encontraba dentro de la esfera de la libertad de expresión, esto puede ser justificado en base a lo estipulado por la Comisión Interamericana de Derechos Humanos donde señala:

"La falta de participación de la sociedad en el conocimiento de información que los afectaría directamente impide el desarrollo amplio de sociedades democráticas exacerbando posibles conductas corruptas dentro de la gestión gubernamental y promoviendo políticas de intolerancia y discriminación. La inclusión de todos los sectores de la sociedad en los procesos de comunicación, decisión y desarrollo es fundamental para que sus necesidades, opiniones e intereses sean contemplados en el diseño de políticas y en la toma de decisiones".[50]

Se contrapone a esto, el caso de Villavicencio, ya que, al ser correos electrónicos del gobierno ecuatoriano, el criterio aplicado es totalmente distinto y al analizar la sanción que se le aplico se entendería que este tipo de información se encuentra fuera del marco de libertad de expresión. La libertad de expresión como bien jurídico

[49] Corte Nacional de Justicia, Sala Especializada de lo Penal Militar, Penal Policial y Transito (13-11-2014). Resolución 134-2104. Juicio No 0826-2012 VR. (Juez Vicente Robalino). Es importante señalar que posterior a este proceso se pidió inmediatamente iniciar uno nuevo, en el sistema del Consejo de la Judicatura para consulta de causas, solo consta lo siguiente: "En la ciudad de San Francisco de Quito, Distrito Metropolitano, el día jueves dos de junio del dos mil dieciséis, a las trece horas y ocho minutos en 1 fojas, y 0 cuerpos, anexa cinco fojas útiles en copias certificadas.- Viene por PETICION DE FORMULACION DE CARGOS interpuesto por el señor doctor Galo Chiriboga Zambrano, Fiscal General del Estado, dentro de la Indagación Previa No. 101-2013, seguida por el presunto delito tipificado en el artículo innumerado 1, agregado al Art. 202 del Código Penal, vigente a la fecha en la que ocurrieron los hechos investigados; y, con fundamento en los artículos 195 y 168 de la Constitución Política del Ecuador y artículos 594 numeral 1, 595 del Código Orgánico de la Función Judicial, solicita se señale día y hora para que se lleve a cabo la audiencia en la que se formulará cargos en contra de JOSE CLEVER JIMENEZ CABRERA (fuero de Corte Nacional); y, FERNANDO ALCIBIADES VILLAVICENCIO VALENCIA: se recibió en la Unidad de Gestión Documental, Sorteos y Archivo de la Corte Nacional de Justicia, la demanda propuesta por FISCALIA GENERAL DEL ESTADO contra JIMENEZ CABRERA JOSE CLEVER, ASAMBLEISTA PROVINCIA DE ZAMORA CHINCHIPE, VILLAVICENCIO VALENCIA FERNANDO ALCIBIADES. Correspondió a la SALA ESPECIALIZADA DE LO PENAL, PENAL MILITAR, PENAL POLICIAL Y TRANSITO con el número 17721-2016-0778." (Corte Nacional de Justicia caso Fernando Villavicencio, 2016) Acceso en: http://consultas.funcionjudicial.gob.ec/informacionjudicial/public/informacion.jsf (10-01-2017)

[50] CIDH. Informe Anual 2001. Volumen II: Informe Anual de la Relatoría Especial para la Libertad de Expresión. Capítulo III, párr. 14.

protegido dentro de este tipo penal informático, juega un rol importante en estos casos, sin embargo, lo que realmente interesa es la punibilidad de sus actos para ser considerado un delito informático. Las incongruencias generadas a lo largo de ambos procesos ponen en tela de duda la eficacia y validez de las normas ecuatorianas aplicadas a este tipo de conductas que como consecuencia han causado incertidumbre.

A lo largo de los años en nuestro país se han presentado algunos casos que se han encasillado dentro de los delitos informáticos, esto de alguna manera ha permitido el avance de herramientas y mecanismos que busquen frenar estos actos ilícitos, entre algunos de los casos conocidos encontramos los siguientes:

1. Caso Emetel 1996, desvió y hurto de dinero bajo la técnica de *rounding down.*[51]
2. Ataques de *phishing*[52] y *carding* a bancos ecuatorianos.
3. Terrorismo Informático (Caso Anonymous Ecuador 2010)
4. Caso Gigatribe 2010.

Estos son los casos que de alguna manera lograron llegar a conocimiento de la sociedad ecuatoriana correspondiente a materia penal informática, que al encontrarse con un ordenamiento jurídico débil y nuevo en este tipo de ilícitos no tuvieron consecuencias mayores. Sin embargo, los casos que se presentan a mayor profundidad en este capítulo demostrarán las incongruencias y problemas actuales dentro del marco jurídico ecuatoriano para resolverlos eficazmente.

3.2. Metodología de análisis

Como punto de partida, el análisis de un caso como resulta un "método de aprendizaje acerca de una situación compleja que se basa en el entendimiento comprehensivo de dicha situación, el cual se obtiene a través de la descripción del

[51] ROUNDING DOWN o La Técnica del Salami, consiste en introducir al programa unas instrucciones para que remita a una cuenta determinada los céntimos de dineros de muchas cuentas corrientes. Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada, consistente en que las cantidades de dinero muy pequeñas se van sacando repetidamente de una cuenta y se transfiere a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades de una cuenta y se transfiere a otra. (Obtenido en: http://carloslegislacion.blogspot.com/2012/11/definicion-de-diversos-delitos.html 17-01-2017)

[52] Se conoce como 'phishing' (del inglés fishing - pescar) a la suplantación de identidad (en Internet, pero también por teléfono) que persigue apropiarse de datos confidenciales de los usuarios. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. (Obtenido en: http://carloslegislacion.blogspot.com/2012/11/definicion-de-diversos-delitos.html 17-01-2017)

análisis de la situación tomada como u conjunto dentro de su contexto" (Murillo, 2017, pág. 2). A través de esta definición se entiende que el estudio del caso plantea la investigación de las características esenciales de los mismos y nos permite estudiar un tema determinado, siendo en este caso la aplicación de la normativa ecuatoriana para los delitos informáticos y la correcta valoración de los elementos de convicción para sancionar estas conductas.

Para hacer un estudio objetivo de un caso en particular se debe hacer una correcta selección del método adecuado para una investigación que contenga todos los elementos de convicción necesarios para ser considerado un delito informático. Dentro de la metodología encontramos el método heurístico, que permite ampliar o confirmar lo que ya se sabe para constituir una estrategia (Murillo, 2017, pág. 4) que sirva para la toma decisiones que tenga como fin, llegar a los gestores de justicia para que tomen acciones que no permitan dejar en la impunidad este tipo de conductas. En base a la utilización de esta metodología se podrá confirmar gracias a todo al marco legal ecuatoriano que existe un incumplimiento del mismo que conlleva a la consecución de un ilícito.

A pesar de tener un método especifico que permita el análisis de un caso en particular existen algunos inconvenientes, que radican en la complejidad de los elementos que posee cada caso. En estos casos en particular, tanto el caso de WikiLeaks como el de Fernando Villavicencio poseen ciertas características particulares que los vuelven totalmente similares, lo que genera la duda de la incongruencia al momento de decidir acerca de esta conducta por parte de los gestores de justicia.

En base a esto puedo asumir que el estudio del caso permite tener un contraste correcto de lo que implica la violación de ciertas normas dentro del ordenamiento jurídico ecuatoriano y que a pesar de poseer normas tipificadas que buscan contrarrestar ciertas conductas, existen casos en particular que se saltan todos los procedimientos y tienen argumentos pocos válidos para proteger la decisión del juez. El ejemplo más claro, son los casos que se ha mencionado con anterioridad a lo largo de este capítulo que teniendo los mismos elementos de convicción fueron catalogados totalmente diferente. (Fundamedios, 2016)

3.3.3. Casos de análisis

Al ser un modo delictivo no tradicional, se muestra como una meta la toma de decisiones adecuadas para la aplicación de la normativa existente. Tal es el caso, que existe una amplia confusión al momento de la aplicación de la doctrina y la normativa referente a los delitos informáticos. (Acurio, 2010) El Código Orgánico Integral Penal, les permite a los jueces y todos los sujetos participantes en esta relación enfrentar de alguna manera este tipo de conductas ilícitas, por que los tipos penales tradicionales no han sido actualizados para consolidar la seguridad jurídica que se espera.

Dentro de este capítulo se realizará el análisis de dos casos que poseen ciertas características particulares que en la actualidad son temas importantes dentro de nuestro ordenamiento jurídico, estos casos son:

1. Caso WikiLeaks – Julián Assange.
2. Caso Fernando Villavicencio.

Como se hace mención a lo largo de este capítulo, ambos sujetos activos defienden su argumento sobre la difusión de los correos electrónicos basados en la libertad expresión, bien jurídico protegido, que en Ecuador ha sido violentado y muchas veces debatido. Lo interesante de estos casos es que, a pesar de argumentar lo mismo, el Estado Ecuatoriano tiene una perspectiva totalmente diferente al decidir respecto a la consecución de este ilícito.

Frente a esta diferencia se ha generado un debate que cuestiona la efectividad de las normas o la posibilidad de la existencia de intereses particulares por parte del estado ecuatoriano sobre la información que posee Julián Assange ya que, por el contrario, en el caso de Villavicencio, se lo reprimió totalmente por la difusión de correos electrónicos que contenía información confidencial del gobierno de la misma manera que lo hizo Julián Assange. De cierta manera se entendería que el ilícito fue el mismo, pero la visión para ejecutar justicia o hacer efectivos los mecanismos existentes no son válidos ni eficaces.

3.3.1. Caso WikiLeaks

WikiLeaks, también considerado como la enciclopedia de los secretos de la corrupción, vulneración de los derechos y comportamientos ilícitos alrededor del mundo. Esta página fue creada en el 2007 donde se puede subir archivos de carácter privado de manera anónima. WikiLeaks es una organización que busca desmentir los

comportamientos de los estados a través de la difusión de información sensible que fue creada por Julián Assange. (Assange, 2015)

A lo largo de la existencia de la página se han colgado más de 10 millones de documentos con información sensible, que son difundidos a través de medios de comunicación de alto impacto alrededor del mundo. WikiLeaks tiene una perfecta autenticidad de sus documentos y un alto índice de resistencia cuando han intentado censurarla (Assange, 2015).

Lo característico de la página es que no posee ningún gráfico, es una página que expresa seriedad absoluta donde predomina el texto. El funcionamiento de este gran sitio web que oferta una apariencia simple acarrea un sistema de organización y funcionamiento bastante especial, también podría ser llamado sofisticado. El funcionamiento de la página, parte de la existencia de documentación de interés público que si a su vez son denunciados o presentados a las autoridades públicas estos podrían ser ocultos por intereses que impedirían su difusión, a partir de esto cualquier persona puede dirigirse al sitio web de la página, donde existe un correo electrónico que le permite depositar la información de manera anónima, es decir, ni siquiera quienes controlan la página tienen información de quien fue la persona que les otorgo toda esa documentación. Toda esta información está protegida por criptografía al nivel de la seguridad de los gobiernos o de los ejércitos alrededor del mundo. (Assange, 2015)

Una vez obtenidos todos los documentos, los editores voluntarios de la página examinan la autenticidad de los mismos y que estos realmente sean de interés público. A partir de esto se comparte los documentos, más una nota periodística que explica la importancia de dicha información y por qué esto es beneficioso para el conocimiento de toda la sociedad. Estos editores, se encuentran alrededor de todo el mundo, para que existe respuesta inmediata mientras que los colaboradores directos son personas pertenecientes a los gobiernos y a los sistemas legales. (Assange., 2014)

Una de las mayores filtraciones de la historia, es la de "Afganistán", donde tres días después de la publicación del video de la matanza provocada por el helicóptero en donde existieron muchas víctimas por los conflictos armados existentes entre Estados Unidos y Afganistán, WikiLeaks se convirtió en un peligro enorme para la "seguridad nacional" de los Estados Unidos de Norte América. Esto debido a la difusión de más de 90 mil documentos que contenían información sobre aliados e información militar sobre

el frente en Afganistán, lo que ponía en riesgo la vida de soldados estadounidense según lo señalaba el gobierno. Sin embargo, Assange mencionaba que él no se iba a contener, ni pararía hasta desmentir a los gobiernos corruptos. (Confidencial, 2010)

La filtración de los documentos diplomáticos o también conocido como Cablegate, genero diferentes reacciones en diferentes países del mundo[53], sin embargo, uno de los ataques más controversiales fue hacia los Estados Unidos, debido a esto el gobierno aseguro que tomaría todas las medidas necesarias para no dejar en la impunidad este crimen, ya que el robo de la información clasificada es un crimen. A pesar de esto existen algunas posturas a favor de Assange, que se ven afligidas por un argumento que recae sobre la protección de un estado de su propia población, ya que al poseer conocimiento público del funcionamiento del sistema diplomático y sus planes pone en riesgo a toda una nación. (Comas, 2016)

Lo que realmente interesa en esta disertación referente a WikiLeaks en la posición del Estado ecuatoriano en la situación, sabiendo que ya son cinco años, los que Julián Assange se encuentra con asilo diplomático en la embajada de Ecuador en Reino Unido. Este tema fue controversial dentro del país, pero el Gobierno siempre manifestó haber analizado delicadamente la petición[54] de Julián Assange predominando los derechos antes de que estos se vean vulnerados. Todo esto se dio paso debido a que el

[53] Entre algunos de los países afectados por la publicación de "Cablegate", a más de estar Estados Unidos involucrados, existieron algunas reacciones por parte de algunos países de Latinoamérica como por ejemplo: Brasil, México, Chile, Argentina, Colombia, Venezuela, etc. Debido a que estas filtraciones realizaban fuertes declaraciones que generaron inconvenientes internos en las diferentes naciones antes mencionadas. Acceso en: (http://www.elcomercio.com/app_public_pro.php/actualidad/impacto-de-wikileaks-latinoamerica.html. Fecha: 17-01-2017)

[54] "Con estos antecedentes, el Gobierno del Ecuador, fiel a su tradición de proteger a quienes buscan amparo en su territorio o en los locales de sus misiones diplomáticas, ha decidido conceder asilo diplomático al ciudadano Julián Assange, en base a la solicitud presentada al señor Presidente de la República, mediante comunicación escrita, fechada en Londres, el 19 de junio de 2012, y complementada mediante comunicación fechada en Londres, el 25 de junio de 2012, para lo cual el Gobierno ecuatoriano, tras realizar una justa y objetiva valoración de la situación expuesta por el señor Assange, atendiendo a sus propios dichos y argumentaciones, hace suyos los temores del recurrente, y asume que existen indicios que permiten presumir que puede haber persecución política, o podría producirse tal persecución si no se toman las medidas oportunas y necesarias para evitarla. El Gobierno del Ecuador tiene la certeza de que el Gobierno Británico sabrá valorar la justicia y rectitud de la posición ecuatoriana, y en consonancia con estos argumentos, confía en que el Reino Unido ofrecerá lo antes posible las garantías o el salvoconducto necesarios y pertinentes a la situación del asilado, de tal manera que sus Gobiernos puedan honrar con sus actos la fidelidad que le deben al derecho y a las instituciones internacionales que ambas naciones han contribuido a forjar a lo largo de su historia común." Texto obtenido del Comunicado No. 042 de la Cancillería Ecuatoriana respecto a la concesión del asilo polito a Julián Assange. (Acceso en: http://www.cancilleria.gob.ec/declaracion-del-gobierno-de-la-republica-del-ecuador-sobre-la-solicitud-de-asilo-de-julian-assange/ 17-01-2017)

fundador de esta página web se encontraba perseguido por gobierno de los Estados Unidos, ya que realizó filtraciones que los afectan directamente, como, por ejemplo: el ataque aéreo a Bagdad en el 2007, registros de la guerra en Irak, etc. (Comas, 2016).

Todo esto ha causado presión jurídica, mediática y diplomática para todos los involucrados, pero el Estado Ecuatoriano vio la necesidad de garantizar los derechos de Assange aun sabiendo que dentro de nuestra normativa la difusión de correos electrónicos con información confidencial es un delito, como se mencionara más adelante. (Universo, 2012).

3.3.2 Caso Fernando Villavicencio:

Fernando Villavicencio, asesor del ex legislador Clever Jiménez, fueron acusados de difusión de información confidencial del estado por el delito de hacking, ya que estos se encargaron de difundir correos electrónicos del presidente de la república y el secretario jurídico Alexis Mera. Sin embargo, al no tener suficientes elementos de convicción estos fueron acusados por diversos tipos penales, entre estos: injurias, revelación de información y por último "espionaje o hackeo". A lo largo de este proceso se realizaron allanamientos a las oficina y casa del antes mencionado. Los contenidos de estos correos electrónico radican en corrupción de la Revolución Ciudadana, delitos de lesa humanidad, etc. (FOCUS, 2016)

Villavicencio se dedicó a demostrar supuestos actos de corrupción que se han venido presentado a lo largo de esta década de gobierno que comprenden desde el año 2007 hasta el 2016. En todos los correos electrónicos se hace alusión a una línea de gastos que jamás fueron fiscalizados adecuadamente. Lo interesante radica, en las secuelas de la difusión de estos correos electrónicos a lo largo de un año donde se han generado grandes cambios plasmados en las actuaciones diarias del gobierno o de la función judicial a lo largo de este proceso en contra de Fernando Villavicencio. A pesar de haber estado preso y luego de vivir en la clandestinidad regreso con fuerza para seguir denunciando actos ilícitos dentro del gobierno, donde existe una persecución que busca amordazar a Villavicencio. (Corrales Tapia, 2015)

El caso de Villavicencio llego a instancias internacionales, la Comisión Interamericana de Derechos Humanos (CIDH). Esta solicitó una explicación al Estado sobre lo ocurrido en proceso penal en contra del antes mencionado, requiriendo si esto se dio en consecuencia de la difusión de correos electrónicos, además de presentar las

pruebas que provocaron que se dicte orden de captura en contra de Villavicencio y solicito a Ecuador el cumplimiento de medidas cautelares[55]. (Corrales Tapia, 2015). En vista de lo antes expuesto el caso de Fernando Villavicencio, sigue siendo foco en la actualidad ya que sigue generando consecuencias dentro del gobierno además de seguir siendo una persona perseguida que en su lucha por la libertad de expresión como el argumenta, se encuentran en riesgo su vida y la de su familia. (FOCUS, 2016)

3.4 Análisis comparativo del caso Fernando Villavicencio VS WikiLeaks:

Para realizar un correcto análisis sobre ambos casos es necesario explicar el alcance de la libertad de expresión como bien jurídico protegido en Ecuador. Aun no se ha logrado conceptualizar en su totalidad lo que comprende un *"bien jurídico protegido"* como lo menciona Roxin en su obra de Derecho Penal "…la cuestión teórica del concepto material de delito sigue sin estar clara, pues hasta ahora no se ha logrado precisar el concepto de 'bien jurídico' de modo que pudiera ofrecer una delimitación jurídicamente fundada y satisfactoria por su contenido" (1994, pág. 54). Por otro lado, se menciona que la conceptualización del bien jurídico cambia respecto a las manos que lo sujetan para transformarlo en algo completamente distinto. (Welzel, , cit. por Günthe Jakobs, 1991, pag 58)

A pesar de las dificultades para lograr conceptualizar, Franz Von Liszt señala que "Nosotros llamamos bienes jurídicos a los intereses protegidos por el Derecho.

[55] "El 24 de marzo de 2014, la CIDH solicitó la adopción de medidas cautelares a favor de Fernando Alcibíades Villavicencio Valencia, Cléver Jiménez y Carlos Eduardo Figueroa Figueroa, en Ecuador. La solicitud de medidas cautelares había sido presentada en el contexto de la petición individual P-107-14, en la que se alegan presuntas violaciones a los derechos consagrados en los artículos 8 (garantías judiciales); 9 (principio de legalidad); 13 (libertad de pensamiento y expresión) y 25 (protección judicial), a la luz de las obligaciones generales consagradas en los artículos 1.1 y 2 de la Convención Americana sobre Derechos Humanos. En particular, los solicitantes requirieron medidas cautelares "con el fin de que el Estado suspenda la ejecución de la sentencia de Casación emitida en su contra el día 14 de enero de 2014, por el daño grave e irreparable que el proceso en sí mismo y la posterior sentencia tendrían en sus derechos a la vida, integridad personal, libertad personal, derechos políticos y libertad de expresión". Durante el procedimiento, el Estado presentó informes en fechas 8 y 28 de febrero de 2014. Por su parte, los solicitantes presentaron informes adicionales en fechas 9 y 27 de febrero de 2014; y, 17 y 19 de marzo de 2014. Tras analizar las alegaciones de hecho y de derecho presentadas por las partes, la Comisión considera que la información presentada demuestra prima facie que los derechos de los señores Fernando Alcibíades Villavicencio Valencia, Cléver Jiménez y Carlos Eduardo Figueroa Figueroa se encontrarían en una situación de gravedad y urgencia y de daño irreparable. En consecuencia, de acuerdo con el Artículo 25 (1) de su Reglamento, la Comisión solicita al Estado de Ecuador que suspenda inmediatamente los efectos de la decisión de 14 de enero de 2014, emitida por el Tribunal de Casación de la Sala Especializada de lo Penal, Penal Militar, Penal Policial y Tránsito de la Corte Nacional de Justicia, hasta que la CIDH se haya pronunciado sobre la petición individual P-107-14" (Acceso en: https://www.oas.org/es/cidh/decisiones/pdf/2014/MC30-14-ES.pdf 17-01-2017)

Bien jurídico es el interés jurídicamente protegido. Todos los bienes jurídicos son intereses vitales del individuo o de la comunidad. El orden jurídico no crea el interés, lo crea la vida; pero la protección del Derecho eleva el interés vital a bien jurídico" (Lizt, 199, pág. 6). Entonces se entiende que el bien jurudico radica en un interes que precisa ser reconocido juridicamente para el bien comun de la sociedad.

Teniendo la idea clara de lo que involucra un bien juridico protegido, se da paso a la conceptualiacion de la libertad, "proviene del latín libertas, que designa el accionar humano" (De conceptos., s.f.). Sin embargo Cabanellas define a la libertad como

"Facultad natural que tiene el hombre de obrar de una manera o de otra, y de no obrar, por lo cual es responsable de sus actos", sin embargo este mismo autor asigna, en el campo jurídico, la siguiente sentencia: "Entendida la libertad como autonomía individual, absoluta en el pensamiento, y mayor o menor según las relaciones surgidas de la convivencia social, ha movido a definiciones de juristas y legisladores. Envuelta en la anonimia, pero aureolada por notable perspicacia jurídica, los romanos decían: "Libertas est potestas faciendi id quod Jure licet" (La libertad es la facultad de hacer lo que el derecho permite)". (Cabanellas, 2006)

Partiendo del contenido general de lo que comprende la libertad se desprende el derecho a la libertad de expresión, que en los casos mencionados a lo largo de este capítulo puede ser comprendido como el bien jurídico protegido que se está violentado. La libertad de expresión es un derecho fundamental señalado en la Declaración Universal de los Derechos Humanos, además de encontrarse en las diferentes cartas magnas alrededor del mundo. Entiéndase a estas libertades, aquellas que se encuentran garantizadas para el bienestar de la sociedad. En el Ecuador dentro de nuestra Constitución se declara a la comunicación como un derecho garantizado para todos y todas las ecuatorianas, sabiendo que dentro del artículo 66[56] de la misma se hace

[56] Sección tercera Comunicación e Información
Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos. 2. El acceso universal a las tecnologías de información y comunicación. 3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas. 4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad. 5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.
Art. 17.- El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto: 1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del

un claro hincapié sobre el derecho a opinar y expresar la opinión libremente en sus formas y manifestaciones. (Arguello, 2015)

Este tema se volvió bastante coyuntural en el Ecuador, debido a que durante este periodo han existido clausuras de medios de comunicación, persecuciones a personas naturales y comunicadores, pero en realidad es un tema que siempre ha estado presente a lo largo de la historia de nuestro país. Sin embargo, esta figura engloba un doble standard debido a que los propios precursores de la misma, de alguna manera han generado censura previa del mismo derecho. La misma ley de comunicación ha generado demasiada polémica ya que genera caos en el actual sistema de comunicación del país, tomando en cuenta que siempre han considerado que la libertad de expresión debe ser regulado como un bien público. (Arguello, 2015)

Entonces se ha manifestado que la libertad de expresión es un derecho inherente a la persona y que su aplicación se deriva de nuestra moral en aplicación a las normas éticas que propone la sociedad y en algunos casos dependerá de la deontología de la carrera profesional específica que precisa de cierta difusión de información. Para validar ese criterio la Corte Interamericana de Derechos Humanos señala:

"La Convención Americana […], en su artículo 13.1 dispone que[,] '[t]oda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho

---

espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo. 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada. 3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias.

Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

Art. 19.- La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos.

Art. 20.- El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación

Art. 66.- Se reconoce y garantizará a las personas:

6. El derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones.

comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección'". También recordó que la Corte Interamericana señaló que, "[e]l artículo 13 señala que la libertad de pensamiento y expresión 'comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole'. Esos términos establecen literalmente que quienes están bajo la protección de la Convención tienen no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole. Por tanto, cuando se restringe ilegalmente la libertad de expresión de un individuo, no sólo es el derecho de ese individuo el que está siendo violado, sino también el derecho de todos a 'recibir' informaciones e ideas, de donde resulta que el derecho protegido por el artículo 13 tiene un alcance y un carácter especiales. Se ponen así de manifiesto las dos dimensiones de la libertad de expresión. En efecto, ésta requiere, por un lado, que nadie sea arbitrariamente menoscabado o impedido de manifestar su propio pensamiento y representa, por tanto, un derecho de cada individuo; pero implica también, por otro lado, un derecho colectivo a recibir cualquier información a conocer la expresión del pensamiento ajeno"[57]

Dentro de este derecho, se desprende el derecho de libertad de prensa que es el que compete directamente a Julián Assange y Fernando Villavicencio. En el sentido más amplio del derecho de libertad de expresión, el núcleo o elemento central, es la libertad de prensa su mayor cimiento, esto se da en razón de que la prensa juega un papel importante en la sociedad al informar sobre temas relevantes que son de conocimiento de la sociedad que algunas veces puede verse amenazado por diferentes tipos de censura. (Melo, 2004). Se debe recordar que, a pesar de ser censurados, la información que estos brinden a la ciudadanía debe ser idónea y veraz.

En este caso, se entiende que la libertad de expresión es un derecho que se encuentra garantizado en nuestra legislación, que a pesar de estar positivizadas se han presentado casos donde no se han aplicado los mecanismos para garantizar el cumplimiento del mismo[58]. La libertad de expresión juega un rol importante en la

[57] Corte I.D.H., La Colegiación Obligatoria de Periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). Opinión Consultiva OC-5/85 del 13 de noviembre de 1985. Serie A No. 5, párr. 69.
[58] Véase: SENTENCIA N.o 047-15-SIN-CC CASO N.o 0009-12-IN, Corte Constitucional del Ecuador, 23-09-2015.

construcción de la democracia ya que permite la diversidad de opiniones y el derecho a difundirlo por diferentes medios. En Ecuador han existido varios momentos en donde se ha violentado este derecho, debido a que el estado se ha encargado de colocar varias limitaciones que no viabiliza este derecho. [59]

A lo largo de este capítulo se han expuesto los antecedentes referentes a los casos de Fernando Villavicencio al igual que el de Julián Assange, donde las consecuencias jurídicas de ambos casos son completamente diferentes pero el delito informático cometido fue el mismo. Al marco del Código Orgánico Integral Penal:

"Artículo 232.- Ataque a la integridad de sistemas informáticos. -La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años."[60]

Respecto ambos casos ninguno de los sujetos, es decir: ni Assange, ni Villavicencio alteraron o destruyeron la información, sin embargo, se especulaba que por el hecho de llegar a obtener estos documentos el fin de ambos era generar daños en los sistemas, sin embargo, tanto en Wikileaks como en el caso de Villavicencio, es de conocimiento público que la información era obtenida, en el caso de Wikileaks por filtraciones o contribuciones que se hacen a la página, donde los editores chequean la veracidad de los documentos y en cuanto a Villavicencio, nunca suspendió o trabo el sistema de correo electrónico al que este supuestamente ingreso. Es importante señalar que ambos sujetos, difundieron información que era de relevancia en los diferentes contextos, el uno haciendo hincapié en el mundo en general, mientras que el otro, al

[59] "En vista de la posición del gobierno ecuatoriano de no acatar el mecanismo de medidas cautelares recomendadas por la Comisión Interamericana de Derechos Humanos (CIDH) en el caso de Cléver Jiménez, Carlos Figueroa y Fernando Villavicencio, así como ante su discurso que puso en entre dicho la legitimidad de la CIDH se vio la necesidad de estudiar los argumentos gubernamentales opuestos a la Constitución de la República, al igual que los principios pro homine, buena fe, pacta suntservanda, soberanía y acceso a la justicia en este suceso". (Acceso en: http://repositorio.uasb.edu.ec/bitstream/10644/5119/1/T2034-MRI-Corrales-Incumplimiento.pdf) Véase: CIDH.Medida cautelar No. 30-14, 2014.<https://www.oas.org/es/cidh/decisiones/pdf/2014/MC30-14-ES.pdf> Consultado el 7 de marzo de 2015.

[60] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. República del Ecuador.

margen de supuestos actos de corrupción dentro del Estado Ecuatoriano, mas no existio daño o deterioro, entre los otros verbos rectores que señala el Código Orgánico Integral Penal.

"Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."[61]

En ambos casos existió la difusión de correos electrónicos que contenían información de carácter confidencial. Assange desmantelaba una supuesta corrupción alrededor del mundo, en especial la cometida por parte del gobierno norteamericano, mientras que Villavicencio inicio una ola de ataques a la supuesta corrupción existente a lo largo del gobierno del presidente Rafael Correa. Tanto Assange como Villavicencio han generado conmoción alrededor del mundo por el contenido de la información presentada y estos argumentan que lo hacen en base al derecho de la libertad de expresión como periodistas y que los gobiernos no pueden ocultar esta información a los ciudadanos, porque de cualquier forma afectan a toda la sociedad y deben ser colocados a conocimiento de la sociedad para no dejar en la impunidad todos estos delitos. (Arguello, 2015)

Assange lucha por una información libre y es perseguido por algunos gobiernos del mundo por la comisión de este delito, sin embargo, el estado ecuatoriano vio la necesidad de garantizar los derechos que iban a ser vulnerados hacia el antes mencionado. Assange menciona que se lo acusa por decir la verdad y difundirla alrededor del mundo, para esto en una entrevista realizada a Julián Assange menciona:

"Lo que intento decir es que el mundo está viviendo un cambio muy profundo, y Google es la entidad que más influencia tiene sobre la esencia de ese cambio y tal vez también sobre la velocidad de ese cambio. Podríamos preguntarnos incluso si Google

[61] Penal, C. O. I. publicado en el Registro Oficial Suplemento No. 180 del 10 de febrero de 2014. República del Ecuador.

no es la empresa más influyente en términos absolutos. De esto no estoy seguro. Hay varias mega empresas que podrían ocupar esa posición, la de ser la más influyente en términos absolutos. Pero al menos, de entre las empresas de comunicación, sí, es la más influyente en términos absolutos. Otras compañías pueden tener mucha influencia, como General Electric, o Raytheon, o Booz Allen Hamilton, o ExxonMobil, o Chevron, pero todas ellas tienen, más o menos, un modelo de negocio estabilizado, y el tipo de influencia que ejercen no es tan evidente. Son muy grandes, sí, pero son estáticas. En cambio, Google está en evolución constante; ha duplicado su valor bursátil entre 2011 y este año, pasando de 200.000 millones de dólares a 400.000 millones… Y su penetración en la sociedad global, en términos de interacción con los individuos, ha aumentado más que la de cualquier otra empresa de gran tamaño." (Assange., 2014)

En base al extracto de la entrevista de Julián Assange y según lo expuesto a lo largo de esta disertación la aparición del internet ha generado grandes retos para toda la sociedad. Por una parte, nos da la facilidad de acceso a información en cualquier parte del mundo sobre varios temas, pero por otro lado pone en riesgo la intimidad de las personas respecto a la información que es colocada en el internet. Es decir actualmente muchos delitos se consuman a través de medios electrónicos (Acurio, 2010), donde a pesar de la existencia de elementos que busquen justificar la consecución de un acto ilícito como lo hace Assange basándose en la libertad de expresión, sigue siendo una conducta antijurídica que no debe quedar en la impunidad.

En cuanto a Villavicencio, quien pretende determinar la corrupción existente en el país a través del portal focus, pagina web, donde se difundieron los diferentes correos electrónicos perteneciente al presidente de la República que contienen información de casos graves cometidos en el país respecto a violación de derechos, además de la violación al debido proceso concatenado al incumplimiento de la cadena de custodia de las pruebas presentadas por fiscalía, donde se dio una orden de prisión. (Basabe-Serrano, 2014). Posterior a la liberación de Villavicencio, este tuvo que vivir en la clandestinidad para garantizar sus derechos, pero este mantiene en pie, la importancia de la difusión de esta información que permitan a la ciudadanía ecuatoriana conocer la verdad sobre la corrupción existente en el país.

En resolución a lo expuesto se genera una figura de doble estándar en cuanto a la decisión judicial para estos casos, sabiendo que el derecho penal no puede ser observado desde un punto que no lo relacione con las fuerzas políticas en la sociedad. En este caso

en específico, el Estado ecuatoriano busco perseguir a un sector de la oposición, mediante la sanción a Villavicencio por un supuesto "hackeo" para que después esta información sea escondida para que no genere problemas en el futuro y generar temor en la sociedad para no enfrentar al gobierno en ocasiones futuras. (Basabe-Serrano, 2014). Entiéndase la existencia de una misma conducta que ha sido valorada de forma distinta, provocando el supuesto de que quizás no se está garantizado los derechos de Assange, sino que se está utilizando a ambos sujetos en base a preferencias circunstanciales, siendo uno, opositor del gobierno actual del Ecuador, mientras el otro posee información política estratégica que de alguna manera resulta beneficiosa para el Estado Ecuatoriano.

La existencia de una figura de doble estándar dentro del país, genera inseguridad jurídica porque del orden jurídico se desprende la justicia y se entiende que este debe ser aplicado de la misma manera para todos, el hecho de que el derecho sea de aplicación general genera seguridad (Cabanellas, 2006), porque le otorga a la sociedad la capacidad de confiar en la norma y en las instituciones estatales que se encargan de garantizar los derechos de las personas y para este caso en particular demuestra la falta de capacidad por parte los gestores de justicia para tomar decisiones judiciales que se ajusten al ordenamiento jurídico existente.

Ambos casos suponen un hito respecto a difusión de información respecto a la democracia, basándonos en lo expuesto con anterioridad, una parte fundamental de la democracia esta cimentada en la libertad de expresión que engloba la difusión de información veraz e idónea que permite a la sociedad conocer la realidad de diversos actos. En ese caso, frente al paradigma que presenta el doble estándar judicial solo queda cuestionar discrecionalmente que es lo que realmente se está tratando de ocultar.

La comisión de este delito informático en el país es la prueba palpable para demostrar que dentro del Ecuador existe un gran problema. Por ellos existe la necesidad de tomar medidas y vías efectivas para que no se vuelvan a presentar discordancias de este tipo que solo producen secuelas negativas. Las causas para la existencia de esta anomia quizás engloban intereses políticos, sin embargo, recaen dentro del sistema judicial ecuatoriano, donde resulta preocupante que los fiscales y jueces que avocan conocimiento en esta materia al momento de dictaminar no poseen conocimientos claros sobre la materia y la mecánica para su correcta aplicación. Definitivamente es necesario la concientización del tema a toda la sociedad ecuatoriana

con el fin de clarificar los limites respecto a la difusión de información en función a los delitos informáticos, siendo el hacker, un sujeto activo del mismo, para conocer los límites que implica la intromisión a la red de internet o excepciones que se pueden presentar en casos como estos.

Finalmente citando al profesor alemán Tiedemann, "la criminalidad informática representa un ejemplo y una justificación actualizada de la siguiente afirmación: una legislación (penal) que no tome en cuenta prácticas ya realizadas o conocidas en otros Estados en y con computadoras estaría desde un comienzo condenada al fracaso y una discusión internacional amplia que compare las diferentes experiencias para acabar con la criminalidad de computadoras sería con justicia la indicada para conseguir este objetivo." (Tiedemann, 1993)

Es evidente que todo lo que engloba los delitos informáticos, como la persecución de los sujetos activos puede tomar tiempo y resultar complicado, pero esto no es justificación para dejarlos en la impunidad, por tal motivo es imperioso tomar medidas efectivas inmediatas para los casos que se lleguen a presentar, tomando como base el avance normativo de otros países en materia penal informática con el único fin de evitar resoluciones judiciales completamente diferentes y además lograr una aplicación adecuada de la normativa que genere confianza, veracidad y certidumbre en los actos ejecutados por los jueces competentes de la materia hacia la sociedad ecuatoriana y no se presenten futuras contradicciones como los casos analizados en el presente capítulo.

Conclusiones:

1. Los delitos informáticos en la actualidad han adquirido una relevancia importante, no solo por parte de los legisladores alrededor del mundo, sino por parte de los sujetos activos, puesto que al ser delitos que pueden ser cometidos en cualquier lugar del mundo ya que no conocen fronteras existe una posibilidad muy alta de que estos queden en la impunidad, por ende, han llamado la atención de varias personas alrededor del mundo generando un acercamiento hacia los sistemas tecnológicos por parte de toda la comunidad internauta que en algunos casos persigue fines negativos, es por esto que la imperiosidad de buscar nuevas medidas como campañas de correcta utilización, un organismo autónomo estatal que se encargue de las investigaciones de este tipo de delito o facilidades para los gestores de justicia frente al acceso de capacitaciones constantes sobre estas conductas podrían ser algunas de las medidas que se puedan tomar para frenar o contrarrestar este tipo de delitos.
2. Los delitos informáticos y todo lo que esto comprende, es una temática que debería ser considerada un poco más dentro del marco normativo y social del país, ya que son un conjunto de conductas que a pesar de encontrarse tipificadas en el Código Orgánico Integral Penal son cometidas con mucha facilidad, pues muchas de estas quedan en la impunidad por lo que se deberían tomar medidas o nuevas formas para que se den soluciones válidas y eficaces para contrarrestar este tipo de ilícitos, empezando por diferentes capacitaciones para los gestores de justicia que son los partícipes directos de estos procesos y campañas para la sociedad ecuatoriana en general donde se induzca a una correcta utilización del internet y las secuelas de lo que comprendería una mala utilización del mismo.
3. La forma en la que se encuentran tipificados los delitos informáticos en el Código Orgánico Integral Penal puede generar algunos problemas de interpretación en los jueces o en los propios ciudadanos, porque si bien

durante la disertación se ha buscado diferenciar entre aquellos delitos informáticos como medio y como fin, esto puede ser una causal de una errónea aplicación de la ley por lo que sería conveniente redactar los artículos de modo que estos puedan ser diferenciados fácilmente, identificando cual es la acción que se encuentra sancionando o a su vez la mala interpretación que puede causar algunos vocablos en esta clase de delitos tomando en cuenta que los delitos de esta clase que llegan a ser conocidos aún son muy escasos.

4. Para que exista eficacia respecto a la punibilidad de estos delitos es necesario que exista un compromiso, no solo nacional sino de carácter internacional a fin de que las normas que comprendan delitos informáticos sean uniformes alrededor de la comunidad internacional, esto generaría seguridad en los usuarios de la información del internet debido a que existiría un ordenamiento jurídico internacional armonizado a las pautas de los organismos internacionales que han intentado disminuir la consecución de esta clase de delitos.
5. No se puede negar que el Ecuador ha intentado frenar estas conductas a través del Código Orgánico Integral Penal, sin embargo, existen otros países latinoamericanos que han tomado iniciativas para desarrollar estrategias para dar un seguimiento a los delitos informáticos, sin olvidar que nuestros país ya cuenta con la entidad que certifica las firmas electrónicas, mensajes de datos y comercio electrónico que de alguna manera es un proyecto que ha buscado regular la información dentro del país en el portal del internet.
6. Detrás de la consecución de estas conductas, se encuentra un sujeto activo, que muchas veces es mal llamado "hacker", mas es necesario llamarlo por la tipología adecuada en cuanto a la clasificación doctrinaria sobre las clases de delincuentes informáticos, debido a que este es uno de los primeros pasos para entender las causas o los fines de la comisión del delito informático, precautelando que en los delitos informáticos como fin, el bien jurídico que se protegerá será la información, aunque para muchos autores esto va de la mano con la intimidad.
7. Los delitos informáticos reflejados en cifras en el país aún son inciertos, ya que si existen denuncias que contemplen esta temática, son muy pocas o a su vez por falta de conocimiento de la sociedad o de interés de los mismos se

impide la persecución de los culpables detrás de un ilícito informático. Sin embargo, como se presentó en esta disertación existieron algunos casos que, si bien llegaron a los juzgados penales, no reflejaron un precedente para casos futuros. Tomando en consideración que el caso de Fernando Villavicencio llego a instancias internacionales por diversas causas, este debería ser una de las principales razones por las que el Estado se enfoque en garantizar la inviolabilidad de los derechos de los usuarios ecuatorianos de la red de internet.

8. Como se demostró en los casos analizados en el tercer capítulo de esta disertación existe un alto riesgo de que el sistema garantista del Derecho Penal de la Tecnología e Información surta efectos efectivos por la incompetencia de los jueces, la falta de un juez natural, violaciones al debido proceso, entre algunos otros limites que se presentan dentro de la legislación ecuatoriana o del proceder de los jueces dentro de los diferentes casos en relación a los delitos informáticos, es por ello que deben existir medidas de control sobre las decisiones de los jueces para que en casos similares no se presenten decisiones totalmente diferentes que generen inseguridad jurídica, tomando en cuenta que si los posibles sujetos activos descubren la imposibilidad de la aplicación de muchas de las normas en nuestro ordenamiento jurídico generaría un aumento en la comisión de estas conductas.
9. Considero que después de realizar la presente disertación a lo largo de los capítulos y con el análisis de los casos propuestos en el último capítulo existe una gran necesidad de profesionales del Derecho especialistas en Derecho Informático, además de profesionales de tecnología que trabajen conjuntamente para disminuir estas conductas ilícitas, donde el estado sea el promotor de espacios de participación y capacitación entre los órganos de justicia y los ciudadanos que busque consagrar, una cultura informática dentro del país que tenga como fin el bienestar de la sociedad ecuatoriana que usa el internet diariamente.

Bibliografía

Aboso Gustavo, E. (2006). Cibercriminalidad y Derecho Penal,. Buenos Aires: Montevideo.

Acurio del Pino, S. (2010). Derecho y Nuevas Tecnologias. Quito: Corporacion de Estudios y Publicaciones.

Acurio, S. (2010). *Perfil sobre delitos informaticos en el Ecuador*. Quito.: Fiscalia General del Estado.

Acurio, S. (2015). *Derecho Penal Informatico*. Quito: Corporacion de Estudios y Publicaciones.

Acurio, S. (06 de ENERO de 2017). *Manual de Manejo de Evidencias Digitales y Entornos Informaticos Version 2.0*. Obtenido de https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf

Aez, J. J. (2010). *Derecho y Nuevas Tecnologias*. Quito: Corporaion de Estudios y Publicaciones.

Amman, L. (1989). Hacker für Moskau. Berlin.

Araujo, P. (2014). Teoria del Delito y de la Pena. *Catedra Universitaria*. Quito.

Arguello, J. (21 de abril de 2015). *¿Qué es la libertad de expresión? ¿ hay libertad de expresión en Ecuador?* Obtenido de https://alonewolf474.wordpress.com/2015/04/21/que-es-la-libertad-de-expresion-hay-libertad-de-expresion-en-ecuador/

Artola, J. (. (2007). *Tráfico de personas: cruce de fronteras, documentos de identidad y principales rutas*. . Mexico.

Assange, J. (09 de Enero de 2015). *WikiLeaks*. Obtenido de https://wikileaks.org/What-is-Wikileaks.html

Assange., J. (07 de Diciembre de 2014). WikiLeaks. (I. Ramonet, Entrevistador)

Ballesteros, M. R. (2014). *Anuario Juridico y Economico Escurialense*. Obtenido de file:///C:/Users/Marìa%20Susana%20Vaca/Downloads/Dialnet-Cibercrimen-4639646.pdf

Balseca, R. (16 de Agosto de 2016). *Diario el Telegrafo*. Obtenido de ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario: http://www.eltelegrafo.com.ec/noticias/judicial/13/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Basabe-Serrano, S. &. (2014). Ecuador: Cada vez menos democracia, cada vez más autoritarismo... con elecciones. . *Revista de ciencia política*, 34(1), 145-170.

Becker, B. y. (1990). *Spectacular Computer Crimes*. Michigan.

Bejarano, E. R. (14 de 12 de 2015). *LOS DELITOS INFORMÁTICOS. TRATAMIENTO INTERNACIONAL*. Obtenido de http://www.eumed.net/rev/cccss/04/rbar2.htm

Bequai, A. (1996.). Delitos relativos a las Computadora. En C. d. Europeas, *Delitos relativos a las Computadoras* (pág. 607.). Bruselas.

Blomm, B. (1990). Spectacular Computer Crimes. Washington: Legal Corporation.

Borghello, C. (2009). *Crimenware: El crimen del siglo XXI.* Eset Latinoamerica.

Cabanellas, G. (2006). *Diccionario jurídico. Heliasta.* Heliasta.

Callegari, N. (1998). Delitos informaticos. En S. Carlos, *Cibercimen y Derecho Penal Informatico* (págs. 54-56). Italia.

Camacho, L. (1997). El delito informático.

Castells, M. (2001). *La Galaxia, Internet.* Barcelona: Plaza y Janes.

Claus, R. (2006). : DERECHO PROCESAL PENAL, Editores del Puerto SRL, Traducción de la 25ª edición alemana de Gabriela Cordoba y Daniel Pastor, revisada por Julio Maier. Buenos Aires: Tercera Impresión.

Comas, M. (2016). El caso WikiLeaks como piedra de toque de la democracia deliberativa de Jürgen Habermas. *Universidad de Islas Baleares*, 1-43.

Confidencial, E. (10 de 08 de 2010). El caso "WikiLeaks" solo confirma el atasco que Estados Unidos tiene el Afganistan. *El Confidencial*.

Corrales Tapia, V. H. (2015). Incumplimiento de los pronunciamientos de la CIDH por parte del Estado ecuatoriano. Caso: Cléver Jiménez, Carlos Figueroa y Fernando Villavicencio). Quito: (Master's thesis, Universidad Andina Simón Bolívar, Sede Ecuador.

Correa, R. (2016). Código Orgánico de Economía Social del Conocimiento e Innovación.

Corte Nacional de Justicia caso Fernando Villavicencio, 17721-2016-0778 (Corte Nacional de Justicia 2016).

Cuenca, A. (02 de mayo de 2014). Delitos Informaticos. Quito, Pichincha, Ecuador.

De conceptos. (s.f.). *De conceptos*. Obtenido de http://deconceptos.com/ciencias-sociales/libertad

El Comercio. (21 de 07 de 2015). Los servicios de 'hacker' y espionaje se ofertan sin restricción en la web. *El Comercio*.

Estado, F. G. (2013). *Reporte de Delitos Informaticos.* Quito.

Fernandez, D. (Febrero de 2016). *Delimitacion del Delito informatico.* Obtenido de Consejos de Derecho: http://www.consejosdederecho.com.ar/63.htm

FOCUS. (22 de AGOSTO de 2016). *FOCUS ECUADOR*. Obtenido de "Villavicencio a veces tiene razón": https://focusecuador.com/alexis-mera-villavicencio-a-veces-tiene-raz%C3%B3n-bcc8d942de83#.7zn3612q7

Fundamedios. (28 de octubre de 2016). Obtenido de http://www.fundamedios.org/alertas/juez-ordena-prision-preventiva-para-periodista-y-exasambleista/

Guerra, B. (2009). Consideraciones para la regulación penal de delito informático. Asturias.

Gutierrez, M. L. (s.f.). Fraude Informatico y Estafa. *Daños virtuales*, 2.

Jara, J. (10 de 07 de 2015). *Desafío Ecuador*. Obtenido de Hacking Team y el dilema: ¿seguridad o libertad?: http://www.desafioecuador.org/hacking-team-y-el-dilema-seguridad-o-libertad/

Jijena Leiva, R. (2006). En *Chile, La proteccion penal a a Intimidad y el Delito informatico.* (pág. 14). Chile.

Lacman, V. (2016). *La pornografia y la Internet.* Obtenido de Terra Jurista: http://www.terragnijurista.com.ar/doctrina/pornografia.htm

Levene, R. (2006). *Introduccion a los Delitos Informaticos, tipos y legislacion.*

Libano Manzur, C. (s.f.). *Los Delitos Informaticos.* Editorial Juridica Cono Sur.

Lima, M. d. (2009). Delitos informaticos como medio o fin.

Lizt, F. V. (199). *Tratado de Derecho Penal.* Madrid: Reus.

López, J. P. (18 de mayo de 2012). *Informatica Forense.* Obtenido de http://www.scoop.it/t/informatica-forense/p/1804377335/2012/05/18/caso-real-ex-novio-instala-un-keylogger

Melo, J. O. (MAYO de 2004). *Banco de la Republica Cultural.* Obtenido de http://www.banrepcultural.org/un-papel-a-toda-prueba/la-libertad-de-prensa

Miguel, A. S. (23 de noviembre de 2016). *8 tipos de hacker que debes conocer*. Obtenido de http://axelsanmiguel.com/8-tipos-de-hackers-que-debes-conocer/

Mirò, F. (2012). *Cibercrimen: Fenomenologìa y Criminologia de la delincuencia en el ciberespacio.* Madrid: Marcial Pons.

Muñoz Conde, F. (2003). Introduccion al Derecho Penal. Buenos Aires: Montevideo.

Muñoz., A. G. (2006). *Expansion e Intensificacion del Derecho penal en las nuevas tecnologias.* Republica Dominicana.

Murillo, J. (09 de enero de 2017). *Universidad Autonoma de Madrid.* Obtenido de http://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/EstCasos_Trabajo.pdf

OEA, D. d. (12 de 07 de 2016). *Organizacion de Estados Americanos*. Obtenido de http://www.oas.org/juridico/spanish/cybersp_legis.htm

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., & Arias-Flórez, M. E.-M. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 41-66.

ONU. (02 de 09 de 1990). *Congreso Sobre Prevencion del Delito y Justicia Penal*. Obtenido de http://www.un.org/es/events/crimecongress2015/

Peña, Helen. (s.f.). Delitos Informaticos, Division de Estudios de Posgrado. Mexico, Mexico.

Peso-Navarro, M. G. (29 de 11 de 2001). Delitos Informaticos. Ecuador.

Possley, M. (16 de noviembre de 2016). *III DIGITAL.* Obtenido de http://iipdigital.usembassy.gov/st/spanish/publication/2009/08/20090804181217jkdm3.750247e-02.html#axzz4UneTtki3

Raul Martin. (abril de 2015). *Empezando a Navegar con la informacion* . Obtenido de https://www.uclm.es/profesorado/raulmmartin/Internet.MetododeNegocios/Tema4.pdf

Registro Oficial. (2013). *Codigo Organico Integral Penal.* Quito: Estudio de Publicaciones.

Resa, C. N. (2005). *Crimen Organizado Transnacional: Definición.* España: Astrea.

Resigner, D. (17 de Noviembre de 2008). *Cnet*. Obtenido de GigaTribe brings private P2P sharing to U.S.: https://www.cnet.com/news/gigatribe-brings-private-p2p-sharing-to-u-s/

Revelo Hector. (2010). *Estadisticas 2010*. Obtenido de Delitos informaticos en el Ecuador: www.abogados.ec/2011/02/estadistica-2010-delitos-informaticos-en-ecuador/

Rovira, E. (2002). Delincuencia informática y fraudes informáticos. Granada: Comares.

Roxin, C. (1994). *Derecho Penal Parte General*. Alemania.

Sacchetto, C. (2005). *El principio de territorialidad. EN: UCKMAR, Víctor, ALTAMIRANO, Alejando Y SERRANO ANTÓN, Fernando."Fiscalidad Internacional", Segunda Edición*, . Madrid, España. : Editorial estudios Financieros.

Salamanca, U. d. (05 de septiembre de 2013). *Universidad de Salamanca*. Obtenido de ¿Que es un perito informatico?: www.diariaum.usal.es/salamandra/informatica.com

Salazar., J. C. (06 de mayo de 2014). *La realidad sobre el tráfico de órganos en el mundo*. Obtenido de BBC MUNDO: http://www.bbc.com/mundo/noticias/2014/05/140403_mexico_trafico_organos_mito_realidad_jcps

Sarzana, C. (1999). Definicion de Delitos Informaticos. En C. Sarzana, *Actos criminogenos a traves de un computador*. (pág. 34).

Sutherland, E. (1943). Poder Economico y Delito. En T. Klauss.

Tellez, V. (1996). *Derecho Informatico*. Ciudad de Mexico: Macgraw Hill.

Tiedemann, K. (1983). La criminalidad económica como objeto de investigación, en cuadernos de Política Criminal. Granada: Antares.

Tiedemann, K. (1983). Poder Económico y Delito. Barcelona: Ariel.

Tiedemann, K. (1993). *Lecciones de Derecho Penal Económico*. España: Promociones y Publicaciones Universitarias.

UNDOC, O. D. (2010). *Manual de Instrucciones para la evaluacion de justicia penl*. Nueva York.

Universo, E. (16 de agosto de 2012). Declaracion de asilo a Jullian Assange, fundador de WikiLeaks. *El Universo*.

Voluntad Digital. (13 de enero de 2017). *Voluntad Digital*. Obtenido de http://www.voluntaddigital.com/suplantacion-de-identidad-y-delitos-en-internet/

Zambrano, C. (Octubre de 2014). Apuntes de Introduccion al Derecho penal. *Sujetos del Delito*. Quito, Ecuador.

Zwicky, E. (2010). Heroes de la revolucion de la computacion. *Publicaciones de sistemas informaticos.*, 487-488.

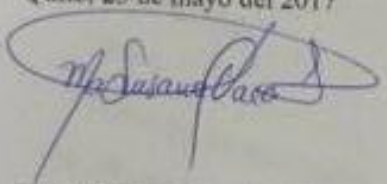
DECLARACIÓN Y AUTORIZACIÓN

Yo, María Susana Vaca Loaiza, con cédula de ciudadanía 110416266-2, autora del Trabajo de graduación titulado: **"EL HACKER COMO SUJETO ACTIVO DEL DELITO, LIMITES Y EXCEPCIONES A LA INTROMISION TECNOLOGICA A LA RED DE INTERNET A LA LUZ DEL CODIGO ORGANICO INTEGRAL PENAL"**, previa a la obtención del grado académico de ABOGADA, en la Facultad de Jurisprudencia:

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENECYT en formato digital una copia del referido trabajo de graduación parea que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Quito, 25 de mayo del 2017



María Susana Vaca Loaiza

CC: 110416266-2

CERTIFICADO DE VOTACIÓN
ELECCIONES GENERALES 2017
2 DE ABRIL 2017

REPÚBLICA DEL ECUADOR

CNE
CONSEJO NACIONAL ELECTORAL

045
JUNTA No.

045 - 145
NÚMERO

1104162662
CÉDULA

VACA LOAIZA MARIA SUSANA
APELLIDOS Y NOMBRES

PICHINCHA
PROVINCIA

CIRCUNSCRIPCIÓN: 3

QUITO
CANTÓN

ZONA:

CUMBAYA
PARROQUIA

REPÚBLICA DEL ECUADOR
DIRECCIÓN GENERAL DE REGISTRO CIVIL, IDENTIFICACIÓN Y CEDULACIÓN

CÉDULA DE CIUDADANÍA No. 110416266-2

APELLIDOS Y NOMBRES
VACA LOAIZA
MARIA SUSANA

LUGAR DE NACIMIENTO
LOJA
LOJA
EL SAGRARIO

FECHA DE NACIMIENTO 1994-05-04
NACIONALIDAD ECUATORIANA
SEXO F
ESTADO CIVIL SOLTERA

INSTRUCCIÓN
SUPERIOR

PROFESIÓN / OCUPACIÓN
ESTUDIANTE

V4343V3242

APELLIDOS Y NOMBRES DEL PADRE
VACA AGUIRRE RAMON ALEJANDRO

APELLIDOS Y NOMBRES DE LA MADRE
LOAIZA MONTERO AMELIA YASMINA

LUGAR Y FECHA DE EXPEDICIÓN
LOJA
2012-06-12

FECHA DE EXPIRACIÓN
2022-06-12

DIRECTOR GENERAL

FIRMA DEL CEDULADO

0005499860